

**DNS in Details: TryHackMe**

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

Date of submission: 16<sup>th</sup> June 2023

## Introduction

In this report, we will delve into the details of DNS (Domain Name System) as covered in the "DNS in Details" module on TryHackMe. We will explore the fundamental concepts and components of DNS, including its purpose, the hierarchical structure of domain names, the various types of DNS records, and the process of making DNS requests. By examining these aspects, we aim to gain a comprehensive understanding of DNS and its role in facilitating internet communication and navigation.

### Task 1: what is DNS

DNS stands for Domain Name System. In simple terms, it is a system that translates human-readable domain names, like "[www.tryhackme.com](http://www.tryhackme.com)," into the corresponding numerical IP addresses "104.22.54.228" that computers use to identify and communicate with each other on the internet. It acts as a directory or phonebook of the internet, helping users access websites and other online services by converting familiar domain names into IP addresses that computers can understand. The screenshot below shows the completion of this section.

*Answer the questions below*

What does DNS stand for?

domain name system

Correct Answer

### Task 2: Domain Hierarchy

Domain hierarchy refers to the structure and organization of domain names on the internet. It involves the arrangement of domains into a hierarchical tree-like structure, with the root domain at the top, followed by top-level domains (TLDs), second-level domains, and subdomains. This hierarchy helps in organizing and categorizing websites based on their purpose, location, or

organization, making it easier to navigate and manage the internet. See the screenshot below for the completion of this section.

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?

ccTLD

Correct Answer

### Task 3: DNS Record types.

DNS record types are specific types of information stored in the DNS (Domain Name System) database. Each record type serves a different purpose and contains specific data related to a domain name. Some common DNS record types include A records for ipv4, AAAA records for ipv6, CNAME record for canonical or alias name for the domain, MX record for mail server and TXT Record for the text fields. The screenshot below shows the completion of this section.

*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 DNS Request

When you make a DNS request, your device sends a query to a DNS resolver (usually provided by your internet service provider or configured in your device settings). The DNS resolver then checks its local cache for the requested domain name's corresponding IP address. If it doesn't have the information, it forwards the request to other DNS servers in a recursive process until a server is found that can provide the authoritative answer. Once the IP address is obtained, it is returned to your device, allowing it to establish a connection with the desired website or service on the internet. See the screenshot below to show completion of this section.

### Answer the questions below

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

TTL

Correct Answer

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

Recursive

Correct Answer

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

authoritative

Correct Answer

## Task 5: Practical

In this practical part, we are going to use the provided website to make DNS request to answers the questions in this section.

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?

Correct Answer

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

Correct Answer Hint

What is the numerical priority value for the MX record?

Correct Answer

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

Correct Answer

DNS Type  Send DNS Request

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

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

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

Here is completion of the module and sharable link

Link: <https://tryhackme.com/room/dnsindetail>

website.thm?

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 website.thm

Server: 127.0.0.53


Address: 127.0.0.53#53

Non-authoritative answer:

Name: website.thm




Address: 10.10.10.10

user@thm:~\$ nslookup website.thm



## Congratulations

You've completed the room! Share this with your friends:

 [Twitter](#)  [Facebook](#)  [LinkedIn](#)

[Leave feedback](#)

## **Conclusion**

Through the DNS in Details module on TryHackMe, I have acquired a thorough understanding of DNS and its use. I have learned about the significance of DNS in translating domain names into IP addresses, the hierarchical organization of domain names, the different types of DNS records, and the process of making DNS requests. This module has provided valuable insights into the functioning of DNS and its importance in maintaining a stable and efficient internet infrastructure. Overall, it has been a rewarding learning experience that has expanded my knowledge and appreciation of DNS.