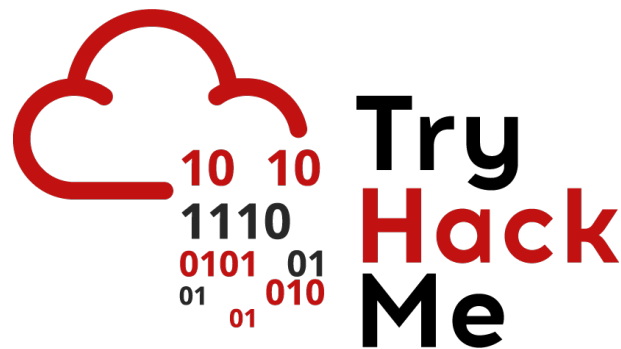


# Writeup: Sala *DNS in Detail*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Sala</b>	<b>2</b>
2.1. Tarea 1 - Qué es DNS? . . . . .	2
2.2. Tarea 2 - Jerarquía de Dominios . . . . .	2
2.3. Tarea 3 - Tipos de Registros . . . . .	3
2.4. Tarea 4 - Realizando una Solicitud . . . . .	3
2.5. Tarea 5 - Práctica . . . . .	4
<b>3. Conclusión sobre la Sala</b>	<b>7</b>

# 1. Introducción

En esta sala aprenderemos sobre los conceptos básicos y avanzados del funcionamiento del **DNS (Domain Name System)**. Además, exploramos cómo se resuelven los nombres de dominio, los tipos de registros DNS más comunes y cómo utilizar herramientas como **dig** y **nslookup** para realizar consultas.

## 2. Sala

### 2.1. Tarea 1 - Qué es DNS?

Aquí nos introducimos al concepto de **DNS (Domain Name System)** donde explica su funcionamiento principal. Después que comprendemos que es DNS, podemos pasar a responder la siguiente pregunta.

**Pregunta:** What does DNS stand for?

**Respuesta:** **Domain Name System**

### 2.2. Tarea 2 - Jerarquía de Dominios

Aquí aprenderemos la estructura jerárquica del sistema DNS, que está organizada en varios niveles donde se detalla como un sistema comienza desde la raíz (**root**), seguido por los dominios de nivel superior (**TLDs**) y después dominios secundarios.

Una vez aprendemos sobre la jerarquía de dominios, pasamos a responder la siguientes preguntas.

**Pregunta:** What is the maximum length of a subdomain?

**Respuesta:** **63**

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

**Respuesta:** **\_** (Respuesta por defecto, hacemos solo clic en **Submit**).

**Pregunta:** What is the maximum length of a domain name?

**Respuesta:** **253**

**Pregunta:** What type of TLD is .co.uk?

**Respuesta:** **ccTLD**

## 2.3. Tarea 3 - Tipos de Registros

Vamos a conocer los distintos tipos de registros DNS donde se explica para qué sirve cada uno. Los registros mas comunes que se destacan son:

- **A**
- **AAAA**
- **CNAME**
- **MX**
- **TXT**

Después que logramos comprender los tipos de registros DNS, vamos a responder las siguientes preguntas.

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

**Respuesta:** **MX**

**Pregunta:** What type of record handles IPv6 addresses?

**Respuesta:** **AAAA**

## 2.4. Tarea 4 - Realizando una Solicitud

En esta tarea conoceremos el proceso de cómo un cliente realiza una solicitud DNS y cómo esta se resuelve paso a paso involucrando distintos servidores con roles diferentes, también, aprendemos los conceptos de **recursividad** y **caché**.

Ahora que entendemos sobre las solicitudes podemos responder las siguientes preguntas.

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

**Respuesta:** **TTL**

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

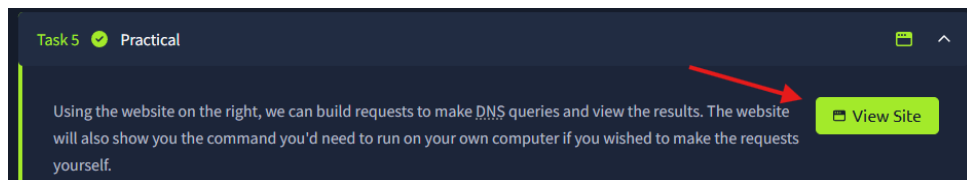
**Respuesta:** **recursive**

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

**Respuesta:** **authoritative**

## 2.5. Tarea 5 - Práctica

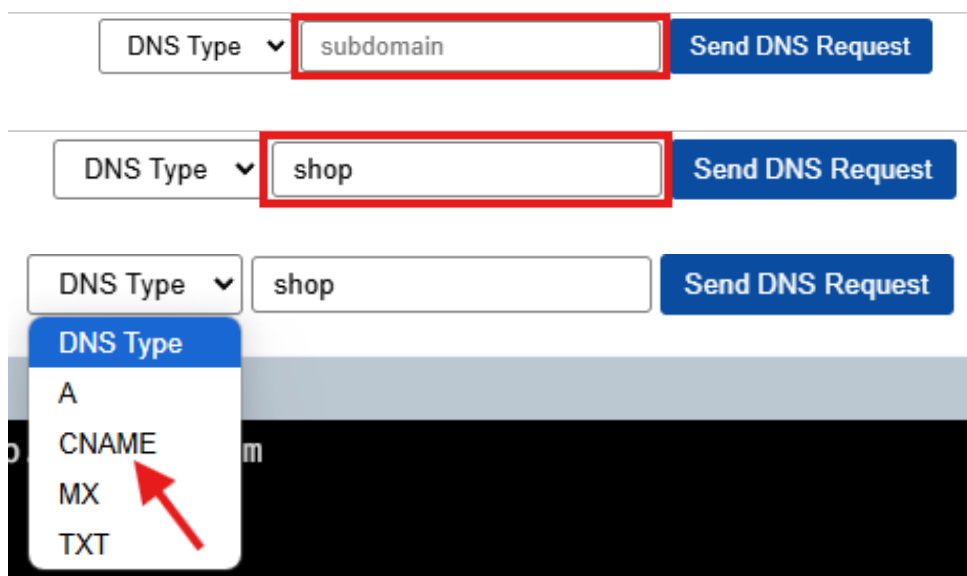
En esta última tarea debemos realizar una práctica de enviar solicitudes DNS para finalizar la sala. Para comenzar, lo primero que haremos es desplegar el sitio donde llevaremos a cabo los ejercicios, haremos clic en **View Site** en el lado superior.

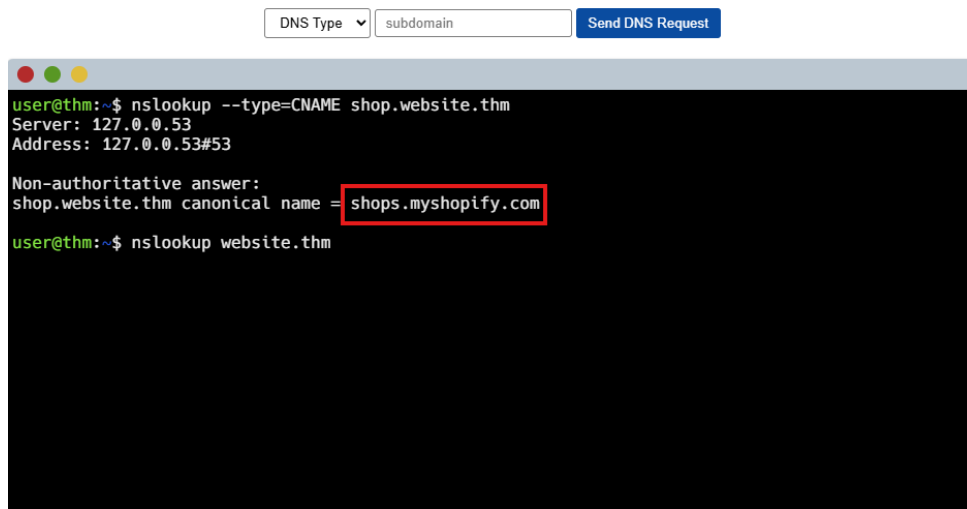


Una vez desplegado el sitio, pasaremos a contestar las siguientes preguntas mediante práctica.

**Pregunta:** What is the CNAME of shop.website.thm?

Para resolver esta primera pregunta debemos dirigirnos al recuadro de texto donde escribiremos **shop**, luego, procederemos a cambiar el tipo de DNS por **CNAME**, posterior a eso vamos a darle a **Send DNS Request**. Nos responderá con el CNAME que buscamos.





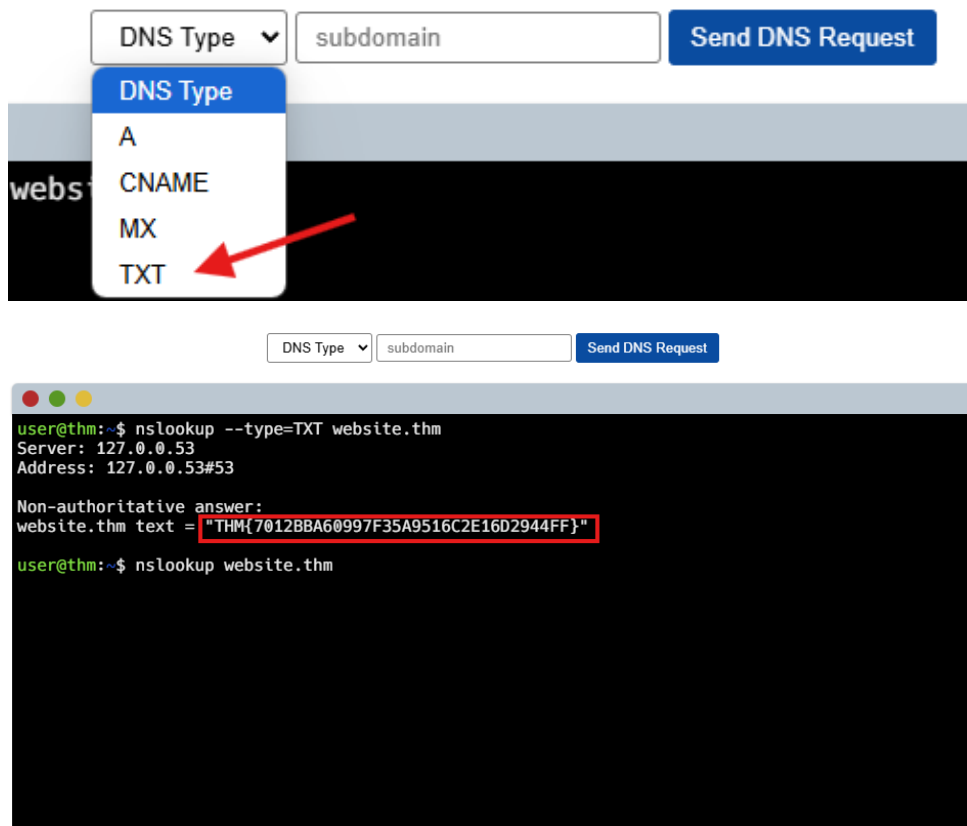
```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com
user@thm:~$ nslookup website.thm
```

**Respuesta:** **shops.myshopify.com**

**Pregunta:** What is the value of the TXT record of website.thm?

Ahora, debemos buscar el valor del registro TXT de website.thm, para ello, solo debemos cambiar el tipo de registro DNS por **TXT** y una vez hecho eso, hacemos clic en **Send DNS Request** y nos responderá con el valor.



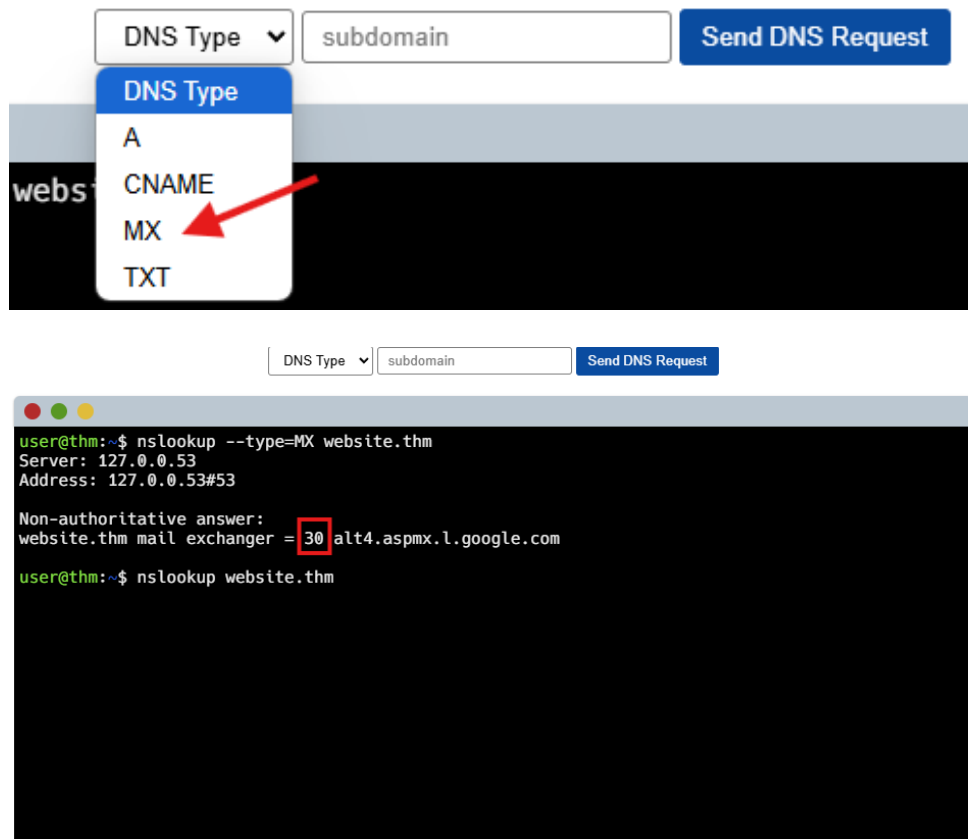
```
user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"
user@thm:~$ nslookup website.thm
```

**Respuesta:** **THM{7012BBA60997F35A9516C2E16D2944FF}**

**Pregunta:** What is the numerical priority value for the MX record? Para conseguir

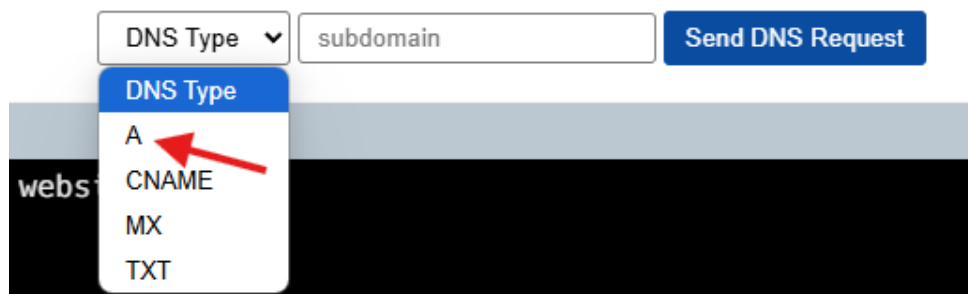
la respuesta a esta pregunta debemos realizar los mismos pasos anteriores, cambiar el tipo de registro DNS por **MX**, hacer clic en [Send DNS Request](#) y nos devolverá con la respuesta a la pregunta.

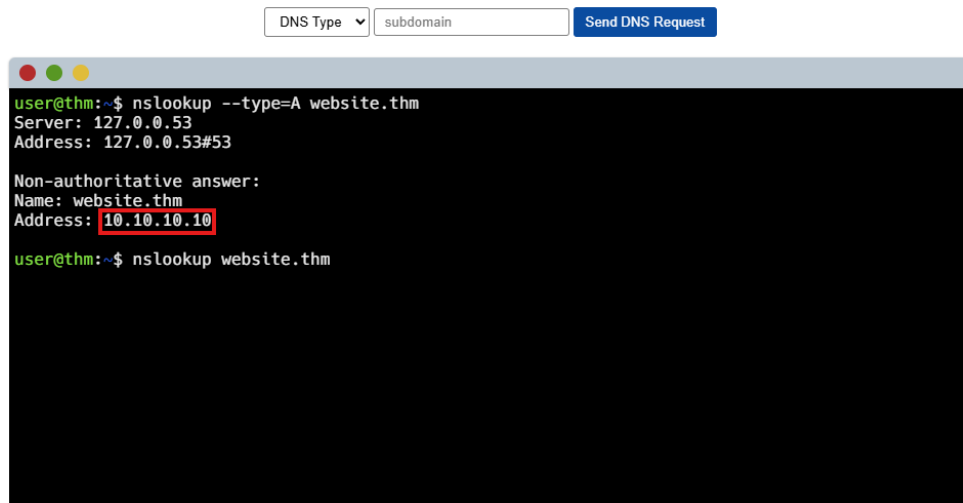


**Respuesta:** 30

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

Para conseguir la respuesta a esta última pregunta tendremos que seguir haciendo los mismos pasos anteriores, esta vez debemos cambiar el tipo de registro DNS a **A**, una vez que cambiamos el tipo de DNS vamos a hacer clic en [Send DNS Request](#) para conseguir la dirección IP del sitio.





The image shows a web interface at the top with a dropdown menu labeled 'DNS Type' set to 'subdomain' and a button labeled 'Send DNS Request'. Below this is a terminal window with the following text:

```
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
```

Respuesta: 10.10.10.10

### 3. Conclusión sobre la Sala

Esta sala logramos obtener conocimiento del funcionamiento del sistema de nombres de dominio, se aprendieron conceptos clave como la jerarquía del DNS, los distintos tipos de registros, el flujo de una solicitud DNS y cómo interactúan los distintos servidores para resolver un nombre de dominio.