Walkthrough Tryhackme Free Roadmap

DNS in Detail

Escrito por:
Ian E. Acosta Sian
Pentester Jr.

Indice

1. What is DNS? **2**
1.1. Respuesta 2

2. Domain Hierarchy **2**
2.1. Respuestas 2

3. Record Types **2**
3.1. Respuestas 3

4. Making A Request **3**
4.1. Respuestas 3

5. Practical **3**
5.1. Respuestas 3

1. What is DNS?

El DNS (Sistema de Nombres de Dominio) nos permite comunicarnos con dispositivos en internet sin tener que recordar direcciones IP complejas como 104.26.10.229. Funciona como una guía que traduce nombres fáciles de recordar (como tryhackme.com) en direcciones IP, similares a direcciones de casas, para facilitar el acceso a sitios web.

1.1. Respuesta

1. What does DNS stand for?
   Respuesta: Domain Name System

2. Domain Hierarchy

La jerarquía de dominios en internet se organiza en varios niveles:

- **TLD (Dominio de Nivel Superior)**: Es la parte final de un dominio, como .com en tryhackme.com. Puede ser:
  - gTLD: genérico, como .com, .org, .edu, .gov.
  - ccTLD: basado en el país, como .ca (Canadá), .co.uk (Reino Unido).
- **Segundo Nivel de Dominio**: Es la parte anterior al TLD. En tryhackme.com, tryhackme es el dominio de segundo nivel. Tiene restricciones como un máximo de 63 caracteres y solo puede usar letras, números y guiones (con algunas reglas).
- **Subdominio**: Es lo que va antes del segundo nivel, separado por un punto. Ejemplo: admin.tryhackme.com, donde admin es el subdominio. También puede haber múltiples subdominios, como jupiter.servers.tryhackme.com, pero el total no debe superar los 253 caracteres. No hay límite en la cantidad de subdominios que se pueden crear.

2.1. Respuestas

1. What is the maximum length of a subdomain?
   Respuesta: 63
2. Which of the following characters cannot be used in a subdomain (3 b _ -)?
   Respuesta: _
3. What is the maximum length of a domain name?
   Respuesta: 253
4. What type of TLD is .co.uk?
   Respuesta: ccTLD

3. Record Types

Existen varios tipos de registros DNS, cada uno con una función específica:

- **A Record:** Asocia un dominio con una dirección IPv4 (ej: 104.26.10.229).
- **AAAA Record:** Asocia un dominio con una dirección IPv6 (ej: 2606:4700:20::681a:be5).
- **CNAME Record:** Redirige un dominio a otro dominio (ej: store.tryhackme.com apunta a shops.shopify.com).
- **MX Record:** Indica los servidores de correo de un dominio, incluyendo prioridades para elegir el servidor correcto si uno falla (ej: alt1.aspmx.l.google.com).
- **TXT Record:** Permite guardar texto libre. Se usa para autorizar servidores de correo o verificar propiedad del dominio, entre otros usos.

3.1. Respuestas

1. What type of record would be used to advise where to send email?
   Respuesta: MX
2. What type of record handles IPv6 addresses?
   Respuesta: AAAA

4. Making A Request

Cuando se hace una solicitud DNS, por ejemplo, al visitar un sitio web:

1. Tu computadora revisa su caché local. Si ya tiene la dirección IP guardada recientemente, la usa directamente.
2. Si no está en caché, se consulta un Servidor DNS Recursivo, normalmente proporcionado por tu ISP o uno que tú elijas. Este también tiene su propia caché.
3. Si el recursivo no tiene la respuesta, inicia una búsqueda desde los servidores raíz de DNS, que lo redirigen al servidor TLD (según el dominio, como .com).
4. El servidor TLD indica cuál es el servidor autoritativo para ese dominio (por ejemplo, kip.ns.cloudflare.com para tryhackme.com).
5. El servidor autoritativo devuelve el registro DNS solicitado (como la dirección IP).
6. El servidor recursivo guarda una copia en caché (según el valor TTL) y envía la respuesta a tu computadora.

4.1. Respuestas

- What field specifies how long a DNS record should be cached for?
  Respuesta: TTL
- What type of DNS Server is usually provided by your ISP?
  Respuesta: recursive
- What type of server holds all the records for a domain?
  Respuesta: authoritative

5. Practical

5.1. Respuestas

1. Para la primera pregunta seleccionamos la opcion **CNAME** y escribimos el subdominio **shop**
   Respuesta: shops.myshopify.com
2. En este caso solo seleccionamos la opción **TXT** y clickeamos **Send DNS Request**
   Respuesta: THM{7012BBA60997F35A9516C2E16D2944FF}
3. Seleccionamos la opción **MX** y enviamos la solicitud
   Respuesta: 30
4. Seleccionamos la opcion **A** para consultar la dirección IP
   Respuesta: 10.10.10.10