Informe laboratorio 3

SERVIDORES DNS

FELIPE LEÓN CÓRDOVA 202173598-4

BENJAMIN LOPEZ 202173533-K

Introducción y propósito del servidor DNS

1. ¿Cuál es el propósito principal del servidor DNS en nuestro sistema?

El propósito principal de los servidores DNS en los sistemas de red actuales es traducir nombres de dominio entendibles por nosotros, como www.ejemplo.com, en direcciones IP numéricas que los computadores utilizan para comunicarse entre sí, como la IP: 93.184.216.34. Esta funcionalidad es crucial para el funcionamiento de internet y de las redes internas, ya que permite a los usuarios acceder a sitios web y servicios en línea mediante nombres fáciles de recordar en lugar de direcciones IP complejas.

2. ¿Cómo podemos utilizar Wireshark para analizar el tráfico de DNS y comprender mejor cómo se utilizan los servicios de DNS en nuestra red?

Wireshark puede ser utilizado para capturar y analizar el tráfico del servidor DNS al filtrar los paquetes que utilizan el protocolo que se utiliza en el servidor el cual es UDP, como también se puede filtrar por la IP del servidor y el puerto que utilizamos. Observando estos paquetes, podemos identificar las solicitudes de resolución de nombres de dominio y las respuestas del servidor, permitiéndonos comprender cómo se resuelven los nombres para obtener las IP que se buscan.

Configuración del servidor DNS

1. ¿Cuál es la configuración básica del servidor DNS (como dirección IP, nombre de host, etc.)?

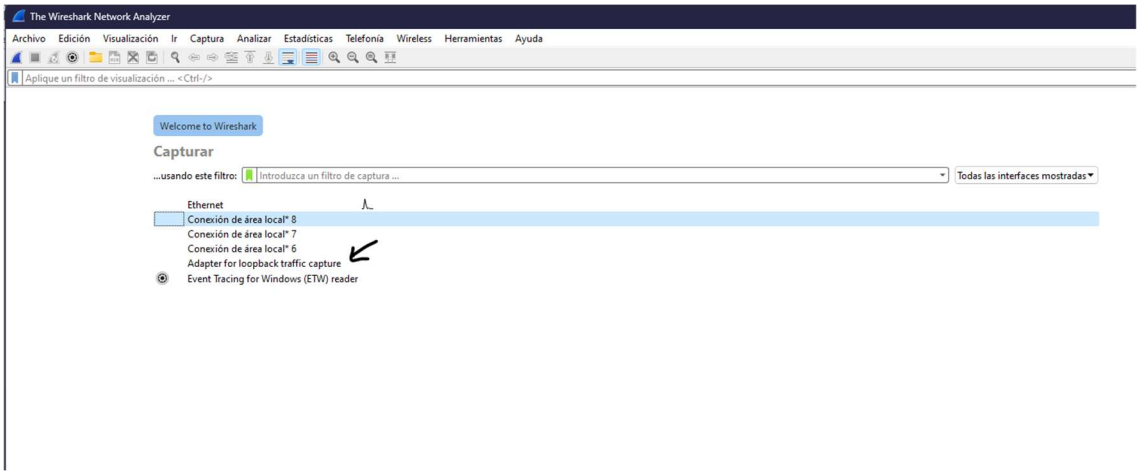
En este caso la conexión básica del servidor DNS la configuramos nosotros debido a que se está estableciendo una conexión local, tanto servidor como cliente son levantados en nuestro computador, distinto sería que el servidor estuviera en otro lado y nos conectáramos a este, habría que adaptar la configuración a los parámetros de este servidor en particular. Nosotros configuramos la IP como localhost y el puerto 63420

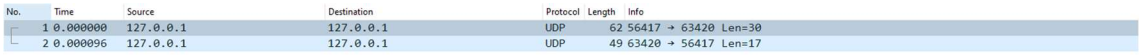
Algunos componentes de la configuración incluyen la dirección IP del servidor DNS, los registros DNS (tipo A, MX, CNAME, NS), nombre del host del servidor DNS el cual facilita su identificación dentro de la red.

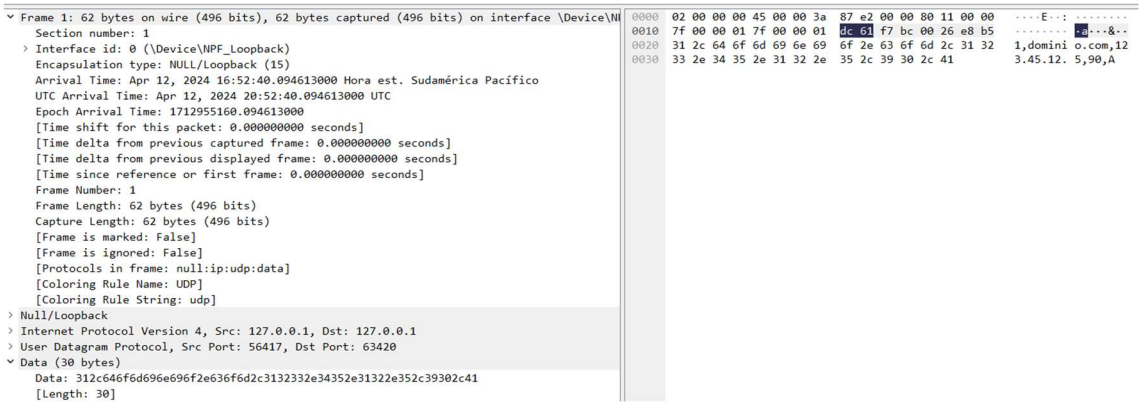
2. ¿Cómo puedo utilizar Wireshark para identificar el tráfico entrante y saliente hacia nuestro servidor DNS, y confirmar su dirección IP y nombre de host?

En Wireshark para poder visualizar el tráfico como se está trabajando con la IP local en este caso de nuestro servidor se debe elegir capturar el tráfico con el filtro “Adapter for loopback traffic capture”, luego mientras Wireshark está capturando el tráfico, cuando se envían mensajes del cliente y este recibe una respuesta del servidor se puede observar toda la información respecto al frame enviado y recibido, el cual se separa en Internet Protocol Version (que posee la IP de origen y de destino del paquete, como también el protocolo

utilizado), User Datagram Protocol (que contiene el puerto de origen y destino) y los bytes de la Data enviada.







Administración de zonas y registros

1. ¿Qué tipos de registros DNS se están utilizando (por ejemplo, A, CNAME, MX, NS)?

El registro tipo A, vincula un dominio con una IP en particular. El registro CNAME consiste en crear un alias para un dominio, esto quiere decir, crear una dirección en la que apunta un dominio en particular, este registro sirve a la hora de tener varios dominios que utilizan el mismo servidor, el registro MX permite indicar a que servidores deben ir los correos electrónicos enviados bajo un cierto dominio en particular y los registros NS en el sistema DNS especifican qué servidores son responsables de manejar las consultas de un dominio específico, direccionando efectivamente el tráfico de internet al hostname de autorización del servidor de nombres para el dominio.

El tipo de registro utilizado en el laboratorio fue el tipo A, esto es evidenciado a la hora en que el cliente entrega un dominio a elección, y se le devuelve a este la dirección IP vinculada.

2. ¿Cuál es el proceso para agregar o eliminar registros DNS en una zona específica?

A la hora de agregar registros primero se debe acceder al sistema de gestión DNS, que este caso es un servidor DNS local, luego debemos ingresar a la zona específica donde se quiera agregar un registro, esto quiere decir al dominio especifico donde deseamos ingresar, seleccionamos la opción de registro que queremos, para un registro A: se necesita el nombre del dominio y la dirección IP correspondiente, para un registro CNAME: se necesita el nombre del host y el nombre de dominio objetivo, para un registro MX: se especifica el nombre del dominio y la dirección del servidor de correo, para un registro NS: se necesita el nombre del dominio y la dirección del servidor DNS autoritativo.

En el caso de este laboratorio fue tipo A al que se hacían consultas, pero al cliente al momento de agregar algún registro se le pedía la IP, nombre de dominio, TTL y Tipo, por lo que podría ingresar lo que cliente desease, pero sólo se realizaban consultas de tipo A para conocer la IP de algún dominio.

Si queremos eliminar un registro debemos acceder a la zona donde queremos eliminarlo, a la hora de encontrarlo lo eliminamos y debemos asegurarnos de que, al eliminarlo, no afecte a la accesibilidad de otros servicios relacionados con este registro.

3. ¿Cómo puedo utilizar Wireshark para capturar y analizar las consultas y respuestas de DNS relacionadas con las zonas y registros específicos de nuestro servidor DNS?

Para utilizar Wireshark en la captura y análisis de consultas y respuestas de nuestro servidor DNS relacionadas con zonas y registros específicos, primero se debe configurar el Wireshark para capturar tráfico en red adecuada (en este caso es localhost). Una vez iniciada la captura, se aplica el filtro UDP para aislar el tráfico pertinente al servidor DNS que fue implementado. Luego, se genera tráfico DNS, ya sea modificando registros en el servidor o realizando consultas desde el cliente, para crear actividad que Wireshark pueda capturar. Finalmente, se analizan los paquetes capturados observando las consultas y las respuestas, prestando especial atención a los tipos de registros y los nombres de dominio para entender cómo nuestro servidor DNS procesa y resuelve las solicitudes.

Conclusión

1. ¿Qué conclusiones podemos extraer de la revisión de la configuración y gestión del servidor DNS?

La revisión del servidor mediante Wireshark muestra que el servidor DNS está configurado adecuadamente para gestionar registros y responder consultas, cumpliendo con su función. Los servidores DNS no solo facilitan la comunicación dentro de las redes al resolver nombres de dominio en direcciones IP, sino que también mejoran la eficiencia operativa al permitir que los usuarios y aplicaciones se comuniquen de manera menos técnica.

2. ¿Cuáles son los puntos fuertes de la configuración actual del servidor DNS y cómo contribuyen a su eficacia en el funcionamiento de la red?

Los puntos fuertes de la configuración del DNS es el manejo dinámico de registros a través de distintos tipos de estos, podemos pasar fácilmente información relevante de un lugar a otro gracias al manejo que nos entrega un servidor DNS permitiéndonos responder a las consultas sobre la IP de cierto dominio con precisión y de manera eficiente para el cliente.

3. ¿Se identificaron áreas específicas que podrían mejorarse en la configuración y gestión del servidor DNS?

Si bien el sistema funciona adecuadamente para los registros de tipo A, siempre es posible mejorar la eficiencia en la respuesta a consultas quizás optimizando como se obtienen los registros almacenados en el servidor en memoria, buscando alguna manera de que esto sea más rápido, aunque se implementó que funcionaran como tipos de diccionarios en donde la llave es el nombre del dominio, otorgando un buen tiempo de respuesta. Otra área que podría mejorarse sería la implementación de medidas de seguridad adicionales, como DNSSEC, que permitiría fortalecer la protección del servidor contra ataques.