Laboratorio 2 Redes de Computadores

Integrantes: Sofía Ríos 202104650-K

Cristóbal Tirado 202104586-4

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

Los servidores DNS colaboran con las consultas realizadas entorno a un dominio en particular, es decir, cuando se consulta por un dominio, el DNS está encargado de traducir este dominio en una dirección IP para luego enviarla a la internet y poder resolver la consulta

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

Para poder ver este tipo de traducciones IP y el posterior ingreso a internet, existe WireShark, una aplicación que visualiza el tráfico de mensajes del computador en tiempo real, en términos del laboratorio realizado, se debe utilizar como filtro de búsqueda “host 127.0.0.1” la cual corresponde a la dirección IP local. Wireshark mostrará el flujo de mensajes que suceden dentro de la red local, por lo que, al momento de correr el código, se mostraran los siguientes mensajes por conexión UDP:

A screenshot of a computer

Description automatically generated

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

La estructura del servidor DNS viene dado por 4 elementos: El dominio, la dirección IP, TTL y el tipo del dominio.

Dominio: es el valor ingresado por el cliente, generalmente son del tipo “algo.com” y este está asociado al registro DNS

IP: es la traducción IPv4 o IPv6 del dominio asociado al DNS, con este valor IP el DNS puede hacer puente entre el dominio consultado y la internet.

TTL: o también conocido como Time to Live, es el tiempo máximo que puede estar el registro DNS del dominio almacenado en la caché del sistema, esto sirve para guardar la consulta hecha y no volver a rehacer la misma solicitud a los servidores DNS.

Tipo: Corresponde a la configuración del dominio que estamos consultando, los tipos de dominio que hemos visto en clases son: A, NS, CNAME y MX.

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

Primero se debe ingresar la IP de local host dentro de WireShark para evaluar en que canal se produce el tráfico de mensajes

A screenshot of a computer

Description automatically generated

Al momento de correr el código hecho, se puede visualizar que en “Adapter for loopback trafic capture” se empieza a producir intercambio de mensajes, entonces es ahí donde se muestra la IP y el nombre del host que, en este caso, es la misma dado que estamos mandando y recibiendo mensajes desde el localhost.

A screenshot of a computer screen

Description automatically generated

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

El código que implementamos es posible agregar dominios al registro DNS del tipo A, NS y MX, dado que nuestro código no reconoce “apodos” al momento de la consulta