CENTRO UNIVERSITARIO
DE TECNOLOGÍA
Y ARTE DIGITAL

Introducción a las redes
PRÁCTICA I (PARTE II)

Los objetivos de esta primera parte de la práctica I son los siguientes:

I. SERVICIO DNS

1. Estudiar el servicio DNS:
    a. Proceso de resolución de nombres mediante el wireshark
    b. Archivo de zona
    c. Registros de recursos
2. Instalación y configuración en Linux del servidor DNS (BIND9)
3. Configuración del cliente DNS.
4. Instalación de un servidor Web en Linux
5. Conexión del cliente para acceder a la página web

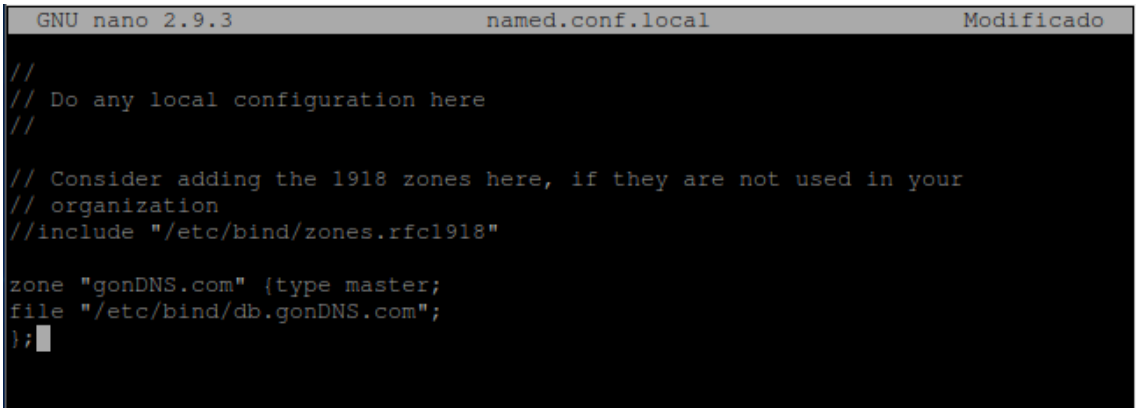
Para ello instalaremos el servicio BIND9 y un servidor http en Linux (Apache o Nginx)

6. Investigar sobre los ataques que pueden sufrir este tipo de servidores

ACTIVIDADES

1. **Instalar un servidor DNS en Linux.**
    a. ¿Cómo funciona y cómo se instala?
        i. Se instala mediante la orden **sudo apt install bind9**
        ii. Configuración del archivo de zona

        iii. Se declara la zona en el fichero **named.conf.local**
        iv. Declaración de la zona y del archivo de zona

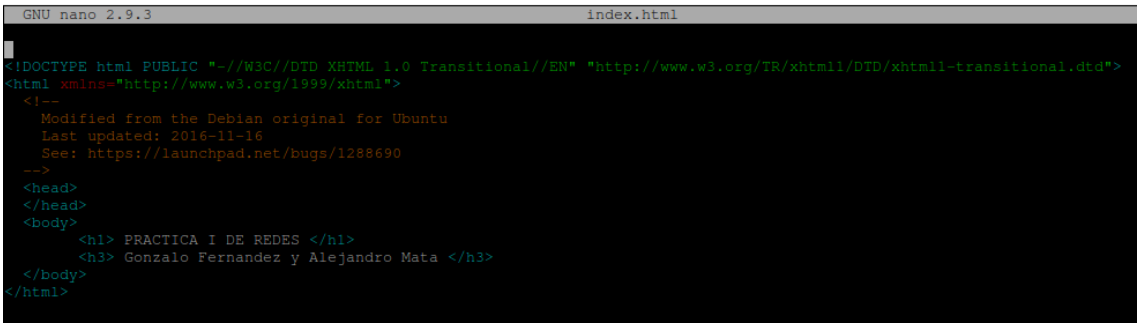


        v. Se reinicia el demonio con la orden **sudo service bind9 restart**

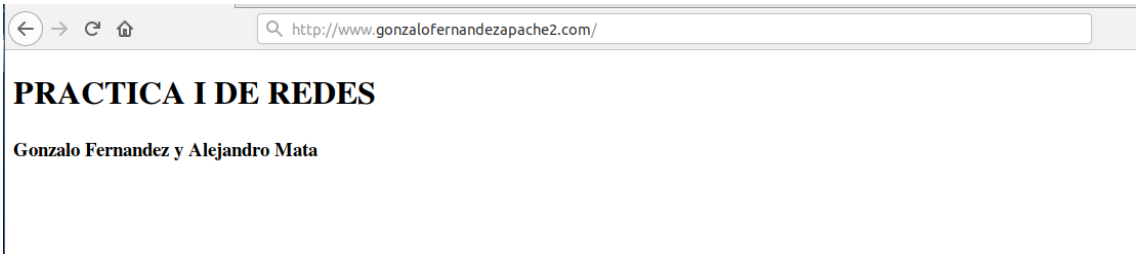
2. **Instalar un servidor Web en Linux (Nginx, Apache o cualquier otro) y publicar una página web de prueba en la que aparezca como mínimo**

el texto "Práctica I de Redes y los nombres de los componentes del grupo"

a. ¿Cómo funciona y cómo se instala?
   i. Se instala mediante la orden **sudo apt install apache2**
   ii. Configuro mi sitio web y la página index en el directorio



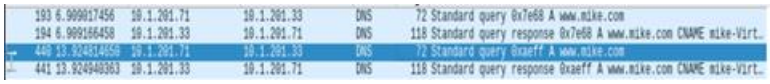
3. **Conexión del cliente a un servidor web mediante la dirección: http://www.midominio.com (ejemplo del nombre; cada uno que ponga el suyo)**



4. **Uso de un sniffer como el Wireshark para:**

a. Identificar los paquetes que intervienen en la resolución de nombres entre el cliente y el servidor DNS

Filtro: dns contains gonzaloFernandezApache2

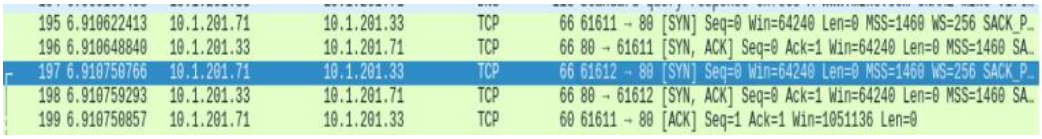


b. ¿Qué protocolo y qué puertos se utilizan en esta resolución, tanto en el cliente como en el servidor? **Protocolos DNS puerto 80**

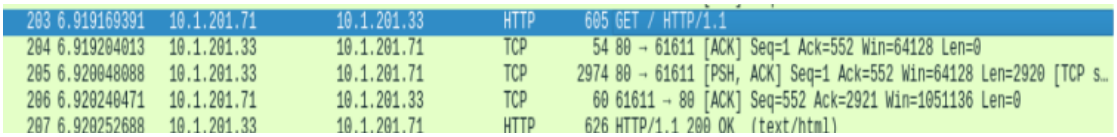
c. ¿Qué tipo de registro de recursos es www? Recordad que hay 6 tipos de registros de recursos.

d. Identificar los paquetes que intervienen en la conexión cliente-servidor web:

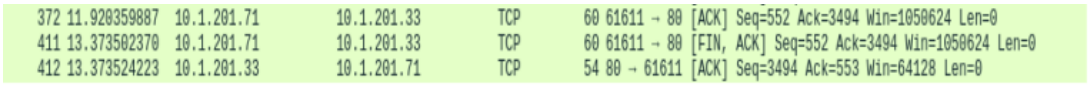
i. Three-way handshake



ii. Obtención de la página web



iii. Fin de conexión



INSERTAR PANTALLAZOS CON LOS PAQUETES FILTRADOS

5. Parte de investigación

a. Investigar y contar brevemente en qué consisten los principales ataques que puede sufrir un servidor DNS. Explicar uno de ellos y buscar un ejemplo real de ataque sufrido por un servidor DNS junto con sus consecuencias **(insertar también algunas referencias de donde hayáis obtenido la información)**

Los servicios DNS son esenciales para navegar a través de la web. Pero es uno de los más vulnerables ante los ataques.

Los ataques DNS más importantes son los siguientes:
Ataque DDos
DNS Spoofing
DNS Hijacking

Vamos a entrar en profundidad en el DNS Hijacking. Este tipo de ataque informático, también reconocido como secuestro DNS, el atacante logra alterar los servidores DNS para que las resoluciones de los nombres fallen y redirijan a la víctima a sitios maliciosos.

De tal forma que el dispositivo de la víctima consulta un dominio "ropa.com", el DNS responde con una IP de un sitio fraudulento y diferente del que buscaba la víctima.

Un caso común suele ser cuando se descarga un archivo de dudosa seguridad e infecta el ordenador, permitiendo al hacker acceder a nuestra configuración de DNS y establecerse como servidor web. Esto le servirá para recibir las solicitudes de acceso a páginas y redireccionarlas a páginas maliciosas.

IMPORTANTE: Si se detecta que esta parte ha sido copiada la práctica será calificada con un 0.

INSTRUCCIONES

- Entrega:
    - Un archivo PDF a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.

- Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo (no hace falta volver a hacerlo si ya se ha hecho para la primera parte de la práctica). **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**

- El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.

- Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.

- **La fecha límite de entrega será el miércoles 4 de noviembre a las 23 horas.**

- No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.