PRÁCTICA 3:
DNS (Domain Name System) CLIENTE

1 Objetivos

En esta práctica se pretende revisar el funcionamiento del servicio de resolución de nombres DNS, desde el punto de vista del cliente.

2 Material

- PC Linux con conexión a Internet, herramientas dig, nslookup, host y whois

3 Requisitos previos

Se recomienda recordar el funcionamiento del servicio DNS (asignatura Redes de Ordenadores). La RFC es http://www.ietf.org/rfc/rfc1035.txt y un resumen interesante está disponible en http://es.wikipedia.org/wiki/Domain_Name_System

4 Herramientas DNS cliente

En el terminal de comandos de Linux hay 3 herramientas principales para hacer funciones de cliente DNS: *dig*, *nslookup*, y *host*. Puede trabajar con cualquiera de ellas (consulte el manual en línea de las mismas) aunque *dig* es la más flexible y moderna. Estas herramientas resuelven nombres de DNS igual que lo hace cualquier otra aplicación de la máquina pero con opciones específicas.

4.1 Compare la dirección IP resuelta por un PING con la de cada una de esas herramientas.

4.2 Si en el navegador web coloca http://www.google.com , descubra la dirección IP que está resolviendo el navegador y si coincide con la resuelta por cada una de estas herramientas.

5 Configuración DNS cliente de una máquina Linux

La búsqueda de un nombre de DNS sigue el orden de búsqueda marcado por /etc/nsswitch.conf en la línea que empieza por “hosts:”. En esta línea se indican los medios de búsqueda en orden para la resolución de nombres, pasando al segundo si no se encuentra en el primero. Por ejemplo, es típico encontrar estos dos medios de búsqueda en este orden:

1- files: se mira el fichero /etc/hosts para buscar el mapeo
2- dns: se realiza la consulta DNS contra el servidor marcado en /etc/resolv.conf

5.1 Compruebe su configuración de /etc/nsswitch.conf, /etc/hosts y /etc/resolv.conf, y deduzca cual va a ser el proceso de búsqueda de nombres en su máquina.

5.2 Determine la dirección IP del servidor o servidores DNS que tiene configurados su máquina

5.3 ¿Qué ocurre si en /etc/resolv.conf hay configurados varios servidores de DNS?

6 Consultas DNS

En este apartado nos centraremos en utilizar la herramienta *dig*.

6.1 Realice una consulta “dig www.unavarra.es” e identifique el significado de cada parte de la respuesta (IN, CNAME, A, QUERY SECTION, ANSWER SECTION, AUTHORITY SECTION, etc).

6.2 Realice las consultas de nombres: unavarra.es, www.unavarra.es ¿Diferencias?

6.3 Con relación al dominio www.navarra.es, averigüe el nombre y dirección IP de los servidores de DNS autoritativos de dicho dominio.

6.4 Realice consultas de DNS de otros nombres de dominio. Identifique los servidores DNS autoritativos de esos nombres de dominio. ¿Por qué normalmente suelen ser 2 servidores autoritativos?

6.5 Realice las consultas de nombres inversas: 130.206.164.68 y de otras direcciones IP que se le ocurran.

6.6 ¿A qué servidor DNS está consultando? ¿Cómo lo puede cambiar sin tocar los ficheros de configuración del sistema?

6.7 Obtenga el registro SOA (Start of Authoriy) del dominio www.navarra.es preguntándoselo al servidor DNS de google 8.8.8.8, y preguntándoselo directamente al servidor primario del dominio www.navarra.es.

6.8 Consulte la dirección IP de www.elpais.com. ¿Cuánto tiempo almacenará en cache su DNS local este registro de recurso? Pregunte varias veces a su DNS local por esta dirección. ¿Qué observa en el TTL del registro de recurso?

6.9 Descubra el TTL de diferentes nombres de dominio de servicios que conozca ¿A qué se puede deber esas diferencias?

6.10 Determine el TTL máximo (original) de un nombre de dominio.

6.11 Averigüe cuantas máquinas (diferentes direcciones IP) están detrás del dominio web www.google.es. ¿Obtiene siempre las mismas y en el mismo orden? ¿Por qué?

6.12 Si elige un servidor DNS que acepte llamadas recursivas, consulte por nombres de dominio raros para comprobar si está ofreciendo funcionalidad de caché o no.

6.13 Pregunte ahora lo mismo a un servidor raíz (por ejemplo J.ROOT-SERVERS.NET) y compruebe en la respuesta si dicho servidor acepta el modo recursivo.

6.14 Haciendo consultas iterativas (opción +norecurse de dig), averigüe la dirección IP de www.timesonline.co.uk. ¿Qué pasos ha dado?

6.15 Puede hacer esto mismo con la opción +trace de dig. Compruebe el resultado que obtiene.

6.16 Utilizando la información disponible a través del DNS determine (nombre y dirección IP) la máquina o máquinas que actúan como servidoras de correo del dominio tlm.unavarra.es.

6.17 Puede obtener los registros AAAA de www.facebook.com ¿A qué corresponden?

6.18 Repita una resolución de DNS capturando la petición y respuesta con Wireshark. Interprete la captura con la petición/respuesta obtenidas en el terminal.

7 Whois y registro de dominios

7.1 Determine el dueño de determinado nombre de dominio sanfermin.com mediante la herramienta whois. Identifique los diferentes tipos de contacto que le suministra el whois y la información que provee de los mismos. Tenga en cuenta que toda esta información es pública e incluye. Inténtelo para sanfermin.es y otros nombres de dominio por los que tenga curiosidad.

7.2 ¿Cuál es el procedimiento para registrar un nombre de dominio a su nombre para utilizarlo en su proyecto y qué infraestructura necesita? Identifique la labor de la entidad registradora de dominios.