

U-TAD

Redes de Ordenadores

Entrega 2

---

## Servicio DNS

---

*Autor*

Gerardo Escudero López  
Ekaitz Arriola Garcia

*Asignatura supervisada por*

Rafael Socas Gutierrez

November 21, 2020

## Problema 1

Instalar un servidor DNS en Linux

(a) ¿Cómo funciona y cómo se instala?

Se instala mediante la orden `sudo apt install bind9`

### Configuración del archivo de zona

```

1  $TTL      604800
2  @        IN      SOA      ns.madrid.org. admin.madrid.org. (
3                      2      ; Serial
4                      604800  ; Refresh
5                      86400   ; Retry
6                      2419200 ; Expire
7                      604800 ) ; Negative Cache TTL
8  ;
9
10 madrid.org. 120      IN      NS       ns.madrid.com.
11 ns.madrid.org. 120    IN      A        192.168.1.51
12 madrid.org. 120     IN      A        192.168.1.51
13 www.madrid.org. 120   IN      A        192.168.1.51

```

Se declara la zona en el fichero `named.conf.local`

### Declaración de la zona y del archivo de zona

```

1  zone "madrid.org" {
2      type master;    //para esclavo type slave;
3      file "/etc/bind/db.madrid.org";
4      //allow-transfer { x.x.x.x } ; //DNS Secundario
5      //also-notify {x.x.x.x}; //DNS SECUNDARIO
6      //lo de arriba lo cambiamos por master{IP DNS primario}
7  };

```

Se reinicia el demonio con la orden `sudo service named restart`

También servirá `sudo service bind9 restart` pero estaríamos reiniciando el super demonio del DNS, que a su vez también reinicia el demonio named.

## Problema 2

Instalar un servidor Web en Linux (Apache) y publicar una página web de prueba

(a) ¿Cómo funciona y cómo se instala?

Se instala mediante la orden `sudo apt install apache2`

Se configura el sitio web y página index en el directorio `/var/www/html`

## Problema 3

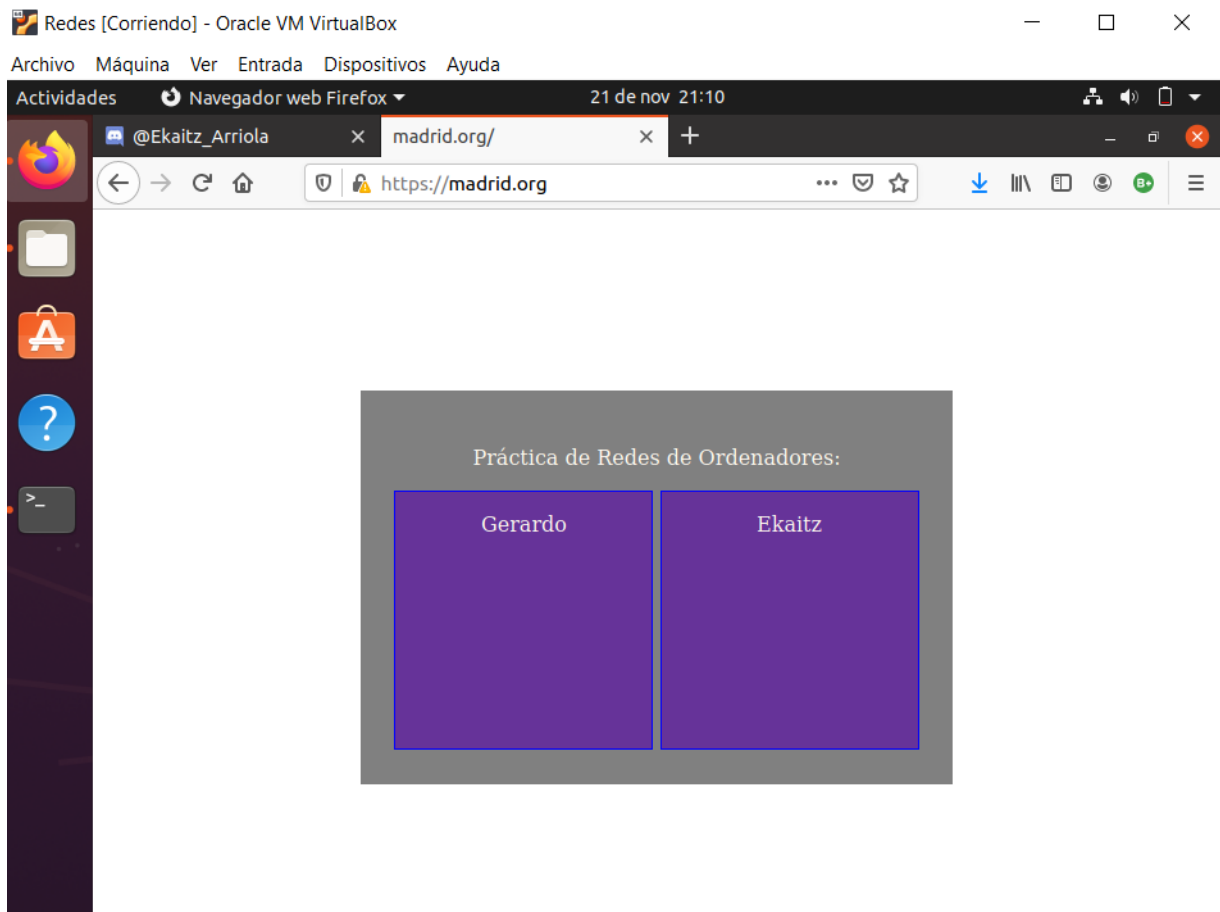


Figure 1: Conexión del cliente a un servidor web mediante la dirección: <http://www.madrid.org>  
Los cuadrados se agrandan si se les hace focus :D

## Problema 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 mediante un ejemplo.

(b) ¿Qué protocolo se utiliza en esta resolución?

Se utiliza el protocolo UDP

(c) ¿Qué tipo de registro es www?

Es un CNAME

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

### i. Three-way handshake

**NO HAY** Three-way handshake ya que nuestra conexión es sobre UDP, aunque es cierto que se puede configurar para que sea sobre TCP. La razón tras hacerlo sobre UDP no es otra que hacerlo más rápido, precisamente al no realizar el Three-way handshake.

Por otro lado, al definirle forwarders al DNS, Firefox sí que intenta hacer unos ajustes rápidos antes de encenderse, estos son, cargar los sitios más buscados como sugerencias y poner una imagen sobre ellos bajo la barra de búsqueda. Para esto necesita las IPs de estos sitios web por lo que la consulta deseada (en este caso "madrid.org"), no será la primera que aparecerá al filtrar con wireshark, sino que estará hundida entre muchas otras.

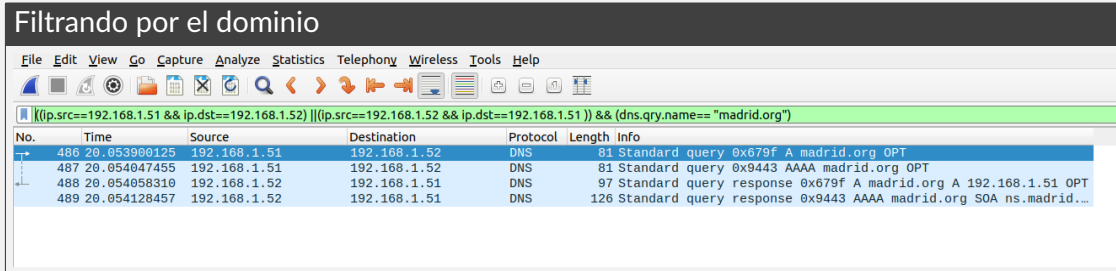
Pero se puede solucionar filtrando por el dominio buscado.

Peticiones DNS entre ambas maquinas antes de filtrar por query

No.	Time	Source	Destination	Protocol	Length	Info
16	3.745536335	192.168.1.51	192.168.1.52	DNS	100	Standard query
18	3.770062913	192.168.1.51	192.168.1.52	DNS	82	Standard query
20	3.781489094	192.168.1.51	192.168.1.52	DNS	109	Standard query
24	3.784580379	192.168.1.52	192.168.1.51	DNS	324	Standard query
25	3.784633961	192.168.1.52	192.168.1.51	DNS	162	Standard query
27	3.790501163	192.168.1.52	192.168.1.51	DNS	194	Standard query
28	4.366224512	192.168.1.51	192.168.1.52	DNS	89	Standard query
29	4.366397911	192.168.1.52	192.168.1.51	DNS	160	Standard query
30	4.709870024	192.168.1.51	192.168.1.52	DNS	108	Standard query
31	4.709968894	192.168.1.52	192.168.1.51	DNS	195	Standard query
32	4.845835603	192.168.1.51	192.168.1.52	DNS	100	Standard query
33	4.845933737	192.168.1.52	192.168.1.51	DNS	184	Standard query

## ii. Obtención de la página web

Filtrando por el dominio



The image shows a Wireshark packet capture window with a filter applied: `((ip.src==192.168.1.51 && ip.dst==192.168.1.52) || (ip.src==192.168.1.52 && ip.dst==192.168.1.51)) && (dns.qry.name=="madrid.org")`. The packet list shows four DNS packets:

No.	Time	Source	Destination	Protocol	Length	Info
486	20.053900125	192.168.1.51	192.168.1.52	DNS	81	Standard query 0x679f A madrid.org OPT
487	20.054047455	192.168.1.51	192.168.1.52	DNS	81	Standard query 0x9443 AAAA madrid.org OPT
488	20.054058310	192.168.1.52	192.168.1.51	DNS	97	Standard query response 0x679f A madrid.org A 192.168.1.51 OPT
489	20.054128457	192.168.1.52	192.168.1.51	DNS	126	Standard query response 0x9443 AAAA madrid.org SOA ns.madrid...

## iii. Fin de conexión

Sigue sin haber al ser conexión UDP.

## Problema 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.

- **Cache poisoning**

Consiste en modificar la cache dns (la local de la víctima o la del propio servidor DNS) para que redirija a la página que tu desees, principalmente para realizar phishing o procedimientos similares.

- **Ataques DNS basados en botnets (Flood)**

Consiste en utilizar multitud de equipos zombis para saturar el DNS con multitud de peticiones sobre un dominio en concreto, por lo que cuando un usuario legítimo intente acceder el servicio será denegado.

- **Ataque de Dominio Fantasma**

Este ataque no contiene fines maliciosos. Sirve para lograr mantener un dominio obliterrado del DNS activo. Esto se consigue recargándolo continuamente en la cache, prolongando así su TTL (time to live) indefinidamente, y por lo tanto suspendiéndolo en la cache hasta finalizar el ataque.

**ATAQUE MIRAI A DYN:**

Mirai es un reconocido troyano que se valió de numerosos dispositivos IoT infectados para formar una botnet, el cual usó con el fin de inutilizar los DNS de Dyn.

En cuanto a la botnet, se apodero de aquella considerable cantidad de dispositivos fácilmente, ya que tenían las credenciales por defecto, o alternativamente carecían de una configuración lo suficientemente firme. Ejemplos bastante recurrentes lo son cámaras o reproductores DVD.