Departamento de Tecnología Electrónica
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Laboratorio 3
Servicios de red

Enunciados de Prácticas de Laboratorio
Tecnologías Avanzadas de la Información

1. Introducción y objetivos

La duración estimada de esta sesión de laboratorio es de **6 horas**. El propósito general de esta sesión de laboratorio es realizar un despliegue de diferentes servicios entre los equipos de la red virtual. Este despliegue será necesario para realizar el último laboratorio dedicado al *Control de Tráfico* y *Calidad de Servicio*.

Concretamente se instalará un servidor WEB, un servidor FTP y un servidor DNS. Los servicios instalados serán públicos a través del la máquina que hace de puerta de enlace. Para conseguirlo se propone configurar adecuadamente *netfilter* de Linux y realizar el reenvío de tráfico a la máquina que sirve cada uno de los servicios.

Nombre de fichero	Descripción
servidor1.crt, servidor1.pem	Certificado digital con clave pública, clave privada
ev.zip	Clonación simple de la página de enseñanza virtual
ev.us.es.crt, ev.us.es.pem, ca-tai.crt	Certificado digital con clave pública, clave privada y Autoridad de Certificación

Tabla 1. Ficheros necesarios para la realización del laboratorio.

2. Instalación de servicios

Antes de comenzar esta sesión de laboratorio se recomienda instalar el software de la tabla 2 en el equipo indicado.

 Paulino Ruiz de Clavijo Vázquez <paulino@dte.us.es>

Nombre del paquete	Descripción	Ubicación
firefox	Navegador Web	Máquina gateway
filezilla	Programa para transferencias FTP/FTS/SFTP	Máquina anfitrión de Virtualbox y máquina gateway.

Tabla 2. Paquetes recomendados para la realización del laboratorio.

Una vez instalado el software anterior, se instalarán dos servicios en el entorno virtual, un servidor WEB en la máquina *Servidor1* y un servidor FTP en la máquina *Servidor2*. En la distribución de Linux utilizada existen multitud de alternativas para la instalación de ambos servidores de hecho, en la tabla 3 se indican las soluciones más habituales utilizadas para estos servicios.

Tipo de Servidor	Nombre del paquete	Página oficial
WEB	apache2 (★★★)	https://httpd.apache.org/
	lighttpd	https://www.lighttpd.net/
	nginx	https://nginx.org/
FTP	proftpd-basic (★★★)	http://www.proftpd.org/
	vsftpd	https://security.appspot.com/vsftpd.html
	pure-ftpd	https://www.pureftpd.org/

Tabla 3. Servidores de uso común en Linux.

Independientemente de las opciones que se escojan, la configuración de los servicios se pueden consultar en la documentación disponible para cada uno de los programas. Se deben escoger dos de ellos a libre elección del alumno y en caso de encontrar alguna dificultad se puede cambiar a alguna otra de las alternativas indicadas en la tabla.

2.1. Instalación de un servidor Web con soporte SSL

Respecto al servidor WEB se deben ofrecer 2 servicios: uno en el puerto estándar HTTP (puerto 80) para páginas sin conexión segura, y otro para HTTPS (puerto 443) donde se servirán páginas seguras usando SSL. Para la puesta en marcha de este servicio realice los siguientes pasos:

Tarea 1.- Instale un servidor WEB (recomendado *apache2*) en la máquina *Servidor1*. Compruebe tras la instalación que hay un programa escuchando en el puerto 80, use el comando `ss -ltnp` e interprete correctamente la salida.

T1.1.- Desde la máquina *Gateway* navegue con Firefox y verifique si aparece una página WEB en la dirección http://192.168.7.100.

T1.2.- La página Web que se está sirviendo está en la ubicación /var/www/html. Cambie dicha página de forma que cuando se navegue aparezca un mensaje de bienvenida con su nombre, del tipo "B*ienvenido al servidor web de Ana*".

T1.3.- El siguiente paso es activar SSL en el puerto 443 utilizando una configuración básica predeterminada. Para activar el soporte SSL con *apache2* debe, en primer lugar, activar el módulo SSL mediante la ejecución del comando `a2enmod ssl`.

T1.3.1.- Tras esto, en el directorio /etc/apache2/sites-available existe un fichero con un ejemplo de configuración SSL, debe enlazarlo o copiarlo al directorio /etc/apache2/sites-enabled.

T1.3.2.- Copie los ficheros `servidor1.crt` y `servidor1.pem` suministrados con el material del laboratorio a `/etc/apache2` y edite el fichero de configuración SSL de apache copiado en la tarea anterior. Establezca correctamente el certificado digital y la clave privada interpretando las directivas de este fichero. Ayúdese viendo con un editor de textos los ficheros `servidor1.crt` y `servidor1.pem`, averiguará cual es el contenido de cada uno de ellos.

T1.3.3.- Tras guardar el archivo de configuración que ha editado, use el comando `apache2ctl configtest` para comprobar si ha cometido errores en la configuración. Debe mostrar sólo una advertencia referente a la directiva *ServerName* que puede ignorar.

T1.3.4.- Tras ello reinicie apache con el comando `systemctl restart apache2`.

T1.3.5.- Verificque de nuevo con el comando `ss -ltnp` que el servidor Web Apache2 está escuchando en el puerto TCP 443.

T1.4.- Navegue desde la máquina *Gateway* a la dirección http://192.168.7.100 y compruebe si funciona el servidor. Tras esto navegue usando SSL (protocolo HTTPS) para comprobar que ocurre con los certificados digitales. ¿Sabe interpretar el aviso del navegador?

T1.4.1.- Antes de confirmar la excepción de seguridad en Firefox use el botón `View` para revisar los datos del certificado y ver donde está el problema.

2.2. Instalación de un servidor FTP

Para el servidor FTP cualquiera de las alternativas de la tabla opera de forma similar, sólo cambian los ficheros de configuración. Tras la instalación del servidor FTP podrá comprobar que el servidor opera aceptando conexiones con la identificación de los usuarios existentes en el sistema, considere que esta configuración predeterminada es un potencial agujero de seguridad por diversos motivos:

- La conexión FTP no está cifrada, además el usuario es el mismo que el del sistema, por tanto, si el inicio de sesión es capturado, con esa misma identificación se puede entrar mediante SSH y obtener un *shell* en la máquina.
- Por defecto se sirve como directorio la cuenta del usuario (ruta `/home/nombre_usuario`), pero es posible acceder a todo el árbol del sistema de ficheros, es decir, la conexión FTP no está limitada a la cuenta del usuario que ha accedido.

Independientemente de estos problemas de seguridad se propone la instalación del servidor FTP y el cambio de configuración predeterminada para intentar evitar, en la medida de lo posible, los problemas de seguridad descritos.

Tarea 2.- Puede escoger alguna de las opciones de la tabla 3, aunque se recomienda *proftpd-basic*, para instalar un servidor FTP en la máquina *Servidor2*.

T2.1.- Tras la instalación, repita el comando usado instaló el servidor Web que lista los programas que están escuchando en los puertos TCP del sistema para verificar que el puerto 21 está en escucha por el servidor FTP.

T2.2.- Instale el programa *ftp* en la máquina *Servidor2* para conectarse a sí mismo usándolo del modo: `ftp localhost`. Ejecute el comando `help` para ver los comandos disponibles en el protocolo FTP.

T2.3.- Repita la prueba desde la máquina Gateway usando el programa Filezilla. Debe instalar este

programa previamente.

T2.4.- Añada varios usuarios en la máquina *Servidor2* mediante el comando `adduser`. Compruebe si pueden conectarse realizando pruebas desde la máquina *Gateway*.

T2.5.- Opcional[1]-3a: Usando la documentación del servidor FTP que ha instalado intente activar el soporte STARTTLS para conseguir que la comunicación se cifre. Configúrelo usando los mismos ficheros de certificado y clave usados con el servidor Web.

T2.6.- Usando *Filezilla* conecte con el usuario *tai* y navegue a la raíz del sistema de ficheros de la máquina remota. Entre en el directorio */etc* y compruebe si tiene acceso a algunos ficheros de configuración del sistema.

T2.7.- Desde la máquina Gateway entre por *ssh* en la máquina *Servidor2* con alguno de los nuevos usuarios que creó y compruebe si mediante el comando `sudo su` puede convertirse en administrador del sistema.

En la última prueba se accedió a los archivos de configuración del sistema operativo. Aunque los permisos predeterminados establecidos por la distribución Ubuntu impiden que los usuarios puedan acceder a muchos de ellos, un error del administrador de la máquina en este sentido puede hacer que se pueda acceder a alguno crítico y se viole la seguridad del sistema. Además el sistema permite la conexión por SSH por lo que el usuario puede ejecutar procesos en la máquina, en un servidor en explotación se debe evitar que los usuarios con acceso FTP puedan conectar mediante SSH y obtener un *shell*. De manera opcional se propone aumentar la seguridad del servicio FTP en la siguiente tarea.

Tarea 3.- Opcional-3b: Para aumentar la seguridad se propone en primer lugar configurar el servidor FTP para que enjaule (*chroot*) a los usuarios en su directorio y en segundo lugar, evitar que puedan acceder por SSH. Se propone realizar los siguientes cambios para aumentar la seguridad:

T3.1.- Configure el servidor FTP para que enjaule (*chroot*) al usuario en su directorio personal. Esto, consiste en que el sistema considere que la raíz del sistema de ficheros es un determinado directorio, por tanto, sólo puede acceder a los directorio hijos, pero nunca al directorio padre ni superiores. Busque como se realiza la configuración con la opción *chroot* del servidor FTP y pruébela.

T3.2.- Busque en Internet como deshabilitar el *shell* a determinados usuarios de un sistema Linux.

T3.3.- Tras este cambio intente entrar por FTP y verá que también se ha cerrado el acceso. Debe reconfigurar el servidor FTP para que permita la entrada usuarios sin shell.

3. Configuración de la puerta de enlace

Tras el despliegue de los servicios en la red interna se debe configurar el *firewall* de la máquina Gateway de forma que redirija servicios públicos a los equipos internos que gestionan cada servicio. En la figura 1 se muestra esquemáticamente como debe configurarse el *firewall*.

Esta figura representa la distribución de los diferentes servicios en máquinas de la red, el objetivo en el despliegue de servicios en el laboratorio consistirá en servir cada servicio en una máquina virtual, para ello, es necesario redirigir tráfico desde el *gateway* a los equipos internos. Así, trabajando en la máquina Gateway realice lo siguiente:

1 Puede encontrar instrucciones extra sobre esta tarea al final del documento en C2.

Tarea 4.- Como administrador cree un nuevo fichero en `/root/bin` llamado `servicios.sh` y añada permiso de ejecución al mismo mediante el comando `chmod +x servicios.sh`.

T4.1.- Escriba en las dos primeras líneas del fichero `servicios.sh` lo indicado a continuación:

```
#!/bin/bash

set -x # Modo para depuración del script
set -e # Si hay algún error con esta opción el script se para

# Antes de cargar las reglas, cargo el firewall que tengo en el script
# para reininicar netfilter

./firewall.sh
```

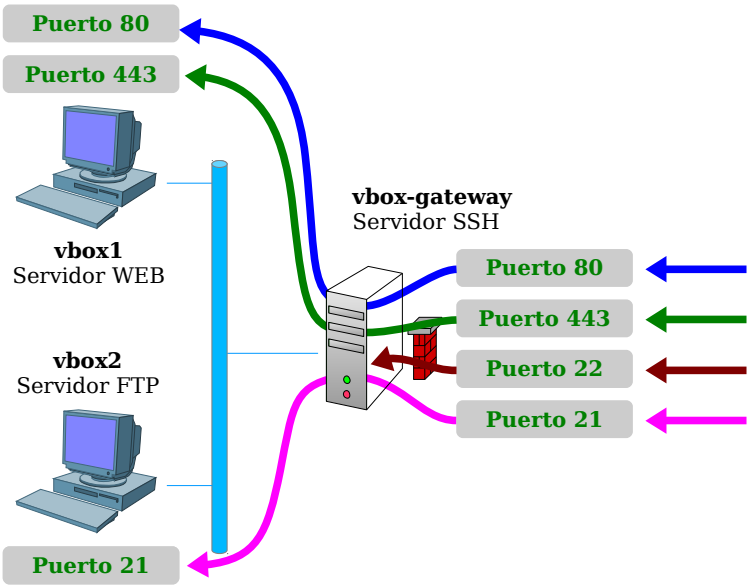

Figura 1. Esquema de configuración del firewall.

Tarea 5.- Trabajando en el fichero `/root/bin/servicios.sh` añada reglas de netfilter para que opere de la forma indicada en la figura 1. Las reglas serán del tipo `-j DNAT` y debe conseguir lo siguiente:

T5.1.- Todo el tráfico que se reciba por la interfaz externa (192.168.20.X) en el puerto 80 debe redirigirse al puerto 80 de la máquina *Servidor1*.

T5.2.- Todo el tráfico que se reciba por la interfaz externa (192.168.20.X) en el puerto 443 debe redirigirse al puerto 443 de la máquina *Servidor1*.

T5.3.- Todo el tráfico que se reciba por la interfaz externa (192.168.20.X) en el puerto 21 debe redirigirse al puerto 21 de la máquina *Servidor2*.

Tarea 6.- Compruebe con un navegador, desde la máquina anfitrión de Virtualbox, o desde otro ordenador del aula, el correcto funcionamiento de la redirección de los servicios, para ello:

T6.1.- Navegue a la dirección http://192.168.20.X

T6.2.- Navegue a la dirección https://192.168.20.X

T6.3.- Use un cliente FTP para conectar mediante ftp://192.168.20.X, es decir, desde un equipo

exterior de la red. Pruebe los modos de operación activo y pasivo ¿funcionan ambos?. Debe intentar transferir ficheros para ver si opera correctamente.

Probablemente el protocolo FTP no esté operando correctamente por estar tras un *firewall*. Para que el protocolo FTP opere correctamente tras el cortafuegos, requiere una configuración adicional, la cual difiere si se utiliza el modo pasivo o activo de FTP. Para facilitar la tarea de configuración, este ejercicio se centra en el modo pasivo. La iteración cliente/servidor en este modo se describe en la figura 2, donde se puede observar el procedimiento de establecimiento de conexión. Una correcta conexión entre el cliente y el servidor FTP requiere la apertura de dos puertos. El procedimiento se puede resumir en los siguientes pasos:

1. El cliente inicia una conexión hacia el servidor en el puerto 21.
2. Una vez establecida la conexión, el cliente indica que quiere pasar a modo pasivo enviando el comando PASV por la conexión previamente establecida.
3. El servidor responde indicando al cliente un número de puerto para que el cliente abra una segunda conexión hacia el servidor usando ese puerto.
4. El cliente establece una segunda conexión con el servidor en el puerto indicado.

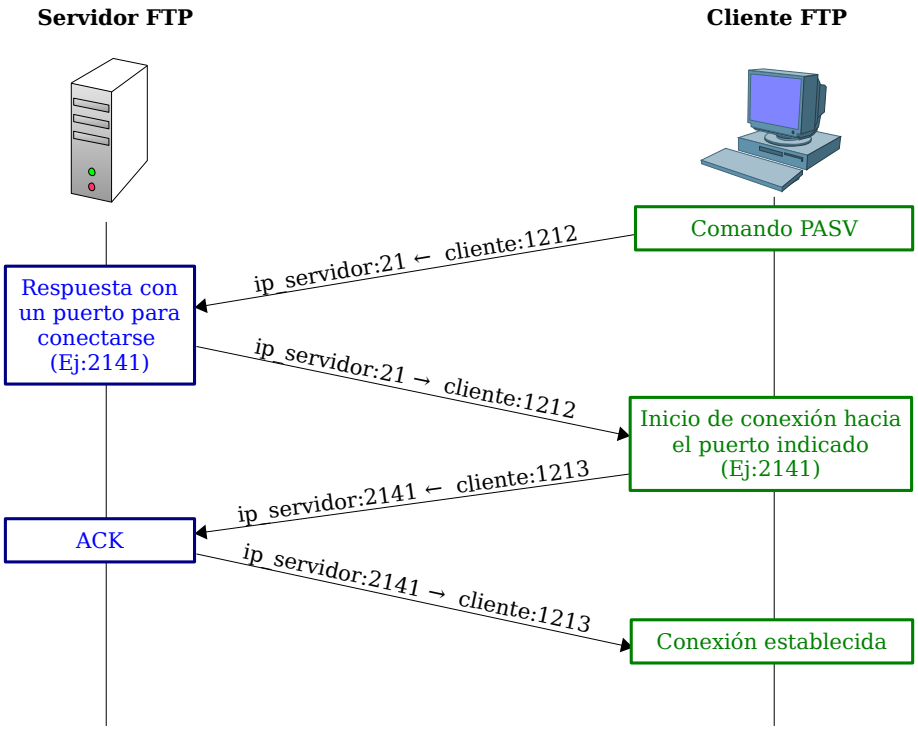

Figura 2. Conexión FTP en modo pasivo.

Cuando el servidor está detrás de un cortafuegos este procedimiento no opera correctamente sin una previa configuración. El principal problema reside en que el *firewall* debe saber que puerto indica el servidor al cliente en el paso 3 para redirigir este puerto al servidor FTP.

Existen multitud de soluciones para este problema, como son módulos dedicados *netfilter* para el protocolo FTP (*ip_conntrack*, i*p_conntrack_ftp* e *ip_nat_ftp*) u otras opciones como la redirección de todos los puertos. En este laboratorio se usará una solución simple, pero que depende en gran medida del servidor FTP usado. Concretamente en la solución propuesta se utilizará *proftpd* y se configurará de

forma que responda al comando PASV del cliente en un rango de puertos definidos por el administrador del servicio FTP. De esta forma sólo habrá que configurar el *firewall* para que redirija este pequeño rango de puertos.

Tarea 7.- Se procederá a configurar el servidor *proftpd* en modo pasivo para un rango de puertos. En caso de usar otro servidor FTP diferente en la documentación del mismo podrá encontrar una configuración equivalente.

T7.1.- En el fichero de configuración /etc/proftpd/proftpd.conf busque las directivas PassivePorts y MasqueradeAddress, debe establecer en ellas un pequeño rango de puertos (del 2000 al 2100 por ejemplo) y la dirección IP externa 192.168.20.X. También debe reiniciar el servicio.

T7.2.- En el *script* servicios.sh debe añadir una regla que redirija el rango de puertos establecidos previamente al servidor FTP. Además, deberá también añadir reglas extra para aceptar esos puertos en el *firewall* ya que está establecida una política prohibitiva de forma predeterminada.

T7.3.- Usando el programa *Filezilla* conecte desde un equipo externo en modo pasivo a su servidor FTP y compruebe si es capaz transferir ficheros.

4. Instalación del servidor DNS

Se pretende instalar un servicio adicional de DNS. La filosofía utilizada a lo largo de la asignatura consiste en realizar un despliegue de servicios mediante un servicio por máquina. Para no saturar los equipos de laboratorio se propone realizar la instalación en la máquina *Servidor2*, junto con el servidor FTP. Concretamente se instalará el servidor BIND9 y este servicio será interno para los equipos de la red virtual.

Para servir peticiones DNS procedentes de la red interna, el servidor DNS operará en modo DNS caché. En este modo el servidor consulta a servidores externos las direcciones IP y las guarda durante un período tiempo para no realizar más peticiones externas cuando se realice la misma petición.

Tarea 8.- Se instalará un servicio DNS cache en la máquina *Servidor2*, para ello, instale en primer lugar el paquete *bind9* en esta máquina.

T8.1.- Edite el fichero /etc/bind/named.conf.options y busque la sección forwarders, que de manera predeterminada está comentada. Quite los comentarios a esta sección y usando la sintaxis correcta establezca las dos siguientes IP como servidores externos: 150.214.186.69 y 8.8.8.8.

T8.2.- Ejecute el comando `named-checkconf` para comprobar si ha cometido errores en la configuración. Si el comando anterior no muestra errores reinicie el servicio *bind9* mediante el comando `systemctl restart bind9` y compruebe si está operativo listando los procesos en ejecución que tienen abiertos puertos UDP (comando `ss -lunp`). ¿Cual es el nombre del programa con el que se ejecuta el servidor *bind*?

T8.3.- Instale el paquete *dnsutils* en todas las máquinas el cual se usará para comprobar el servidor de nombres. Para hacer una peticion directa al servidor de nombres de la Universidad ejecute el comando `dig @150.214.186.69 www.dte.us.es` y observe la repuesta. Repita el proceso con el servidor de nombres 8.8.8.8 y finalmente compruebe si responde su servidor usando la dirección 192.168.7.101.

T8.4.- Si la respuesta es correcta, edite la configuración de todas las máquinas, incluido el *Gateway*,

para que utilicen el nuevo servidor de nombres. Compruebe que opera correctamente en cada máquina para ello use el comando `host` con algún nombre de dominio.

T8.5.- Cambie la configuración del *firewall* en el *script* `firewall.sh` de forma que sólo pueda tener conexión a DNS externos la máquina *Servidor2*. No borre ninguna regla del fichero `firewall.sh`, sólo comente las líneas que no necesite y comente los cambios realizados en el mismo fichero.

T8.6.- Verifique el paso anterior comprobando que el Servidor 1 no es capaz de resolver nombres con ningún servidor externo, para ello use el comando dig con un servidor de nombres externo desde el Servidor 1 y observe el resultado.

4.1. Configuración de un DNS maestro

Para poder disponer de un dominio privado es necesario utilizar un DNS maestro. Dicho servidor será capaz de resolver tanto peticiones de nombres externos (modo servidor DNS caché), como internas. En nuestro caso, el dominio será el nombre del alumno con el sufijo *.tai*. En el ejemplo mostrado se usará por tanto *profesor.tai* y a lo largo del desarrollo del laboratorio debe utilizar su nombre.

El objetivo es conseguir que el servidor de dominio responda con la IP correcta a los dominios mostrados en la tabla 4. Para lograrlo es necesario configurar el servidor DNS en modo maestro para el dominio *profesor.tai*.

Máquina	**Dirección IP**	**Nombre de dominio**
servidor1	192.168.7.100	servidor1.profesor.tai
servidor2	192.168.7.101	servidor2.profesor.tai ns.profesor.tai
gateway	192.168.7.1	profesor.tai gateway.profesor.tai

Tabla 4. Entradas DNS para el dominio profesor.tai.

Tarea 9.- La configuración de un DNS maestro se realiza mediante la edición de varios ficheros. El primer paso es añadir una nueva zona de búsqueda para nuestro dominio, en principio, sólo para búsquedas directas. Edite el fichero `/etc/bind/named.conf.local` y añada una nueva zona usando el dominio *minombre.tai*, para ello básese en el código 1.

```
// Dominio profesor.tai, cambielo por su nombre
zone "profesor.tai" {
        type master;                    // Tipo de servidor
        file "/etc/bind/db.profesor.tai"; // Fichero con los registros DNS
};
```

Código 1. Configuración DNS maestro para una zona.

T9.1.- En el paso anterior se ha especificado un fichero donde estarán las entradas DNS (`db.profesor.tai`) y este fichero no existe puesto que es el nuevo dominio. Debe crear un fichero vacío con este nombre en `/etc/bind` e incluir el contenido mostrado en el código 2, sustituyendo el dominio *profesor.tai* por el dominio que ha escogido. El formato de este fichero es un estándar definido en la RFC1035.

```
; Dominio de laboratorio profesor.tai
; En este fichero los comentarios comienzan con ';'
$TTL    1h                              ; Tiempo de expiracion por defecto
@       IN      SOA     ns.profesor.tai. root.profesor.tai (
                              123456      ; Numero de serie
                              2h          ; Tiempo de refresco
                              10m         ; Tiempo de reintento
                              1w          ; Tiempo de expiracion
                              1h  )       ; Tiempo de Cache TTL
;
@         IN      NS      ns              ; Servidor DNS -> ns.profesor.tai
@         IN      A       192.168.7.1     ; Host principal del dominio -> profesor.tai
@         IN      AAAA    ::1             ; IP version 6 (ipv6)

ns        IN      A       192.168.7.101   ; ns.profesor.tai
servidor1 IN      A       192.168.7.100   ; servidor1.profesor.tai
servidor2 IN      A       192.168.7.101   ; servidor2.profesor.tai
gateway   IN      A       192.168.7.1     ; gateway.profesor.tai
```

Código 2. Entradas DNS para el dominio profesor.tai.

T9.2.- Para revisar si la configuración es correcta hay que utilizar 2 comandos: named-checkconf y named-checkzone. En primer lugar utilice el comando `named-checkconf` para comprobar si ha cometido errores al realizar la configuración. Si no hay errores debe usar el comando `named-checkzone profesor.tai /etc/bind/db.profesor.tai` pero adecuando los parámetros al nombre de zona que ha creado.

T9.3.- Reinicie el servicio mediante el comando `systemctl restart bind9`. Para comprobar si el servicio se ha iniciado correctamente utilice el comando `systemctl status bind9` y revise la bitácora del servicio mediante `journalctl -u bind9`, desplace la bitácora al final y verifique que ha cargado su zona correctamente.

Tarea 10.- Para comprobar si el servidor opera correctamente se probarán diversos comandos. En primer lugar pruebe el comando `host` desde la propia máquina *Servidor2* con las máquinas *servidor1.minombre.tai*, *servidor2.minombre.tai* y *gateway.minombre.tai*.

T10.1.- Repita el proceso desde la máquina *Servidor2* y la máquina *Gateway*.

T10.2.- Use el comando `dig` con *servidor1.minombre.tai*.

T10.3.- Pruebe el comando `ping` con *minombre.tai*, es decir, sin especificar nombre de máquina. ¿que IP resuelve? ¿Por qué ocurre esto?

Tarea 11.- Para conseguir una configuración real de un servidor DNS también es necesario configurar los resolución inversa.

T11.1.- Pruebe el comando `nslookup 150.214.141.196` y obtendrá la resolución inversa ofrecida por los DNS para esta dirección IP.

T11.2.- Pruebe el mismo comando con 192.168.7.100 y obtendrá un error ¿por qué?

T11.3.- Opcional-3c: Consulte documentación sobre cómo configurar BIND9 para la resolución inversa y termine la configuración de su servidor DNS de forma correcta.

4.2. Configuración multidominio

Este último ejercicio consistirá en configurar el servidor WEB para servir páginas diferentes para varios nombres de dominios. Como colofón se realizará un ejercicio de suplantación (*phishing*) mediante

la alteración de entradas de DNS y el servidor WEB. Sólo se mostrará la configuración necesaria con el servidor WEB *Apache.* En caso de haber utilizado *lighttpd* la configuración es similar y la puede consultar por Internet ya que es un servidor WEB ampliamente utilizado.

Tarea 12.- Usando el escritorio de la máquina *Gateway* inicie un navegador de Internet y navegue a http://servidor1.minombre.tai, http://192.168.7.100. Observará que para ambas URLs se está navegando a la misma máquina y se obtiene la misma página WEB.

T12.1.- Navegue ahora a la raíz de su dominio, es decir a http://minombre.tai. Pruebe también http://www.minombre.tai ¿que ocurre?.

T12.2.- Configure correctamente en servidor DNS para que ambos nombres de dominio también se resuelvan con la dirección IP del servidor WEB de la máquina *Servidor1*. Fíjese en el fichero mostrado en el código 2 para resolverlo.

Una vez resuelta la tarea anterior se dispone de 3 nombres de dominio diferentes apuntando a la misma dirección IP. Ahora el objetivo es servir páginas diferentes para cada uno de los nombres de dominio. Apache resuelve esta situación mediante una directiva: *virtualhost*. Esta directiva abre un entorno de configuración donde se pueden definir diferentes opciones para cada nombre de dominio, entre ellas el directorio donde están las páginas WEB para dicho dominio.

Tarea 13.- Como administrador en la máquina *Servidor1* acceda al directorio `/etc/apache2/sites-enabled`. Liste los ficheros y copie el fichero `000-default.conf` como `minombre.conf`. Edite este último fichero para que quede parecido al código 3, debe establecer correctamente todas las directivas resaltadas. En la configuración mostrada se indican los nombres de dominio *minombre.tai* y *www.minombre.tai* mediante las directivas *ServerName* y *ServerAlias*.

```
<VirtualHost *:80>
        ServerAdmin  webmaster@localhost
        DocumentRoot /var/www/minombre.tai
        ServerName   minombre.tai
        ServerAlias  www.minombre.tai
        ErrorLog     ${APACHE_LOG_DIR}/error.log
        CustomLog    ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Código 3.Configuración Virtualhost para apache2.

T13.1.- Una vez establecidos los nombres de dominio *Apache* muestra las páginas WEB situadas en la carpeta indicada mediante la directiva *DocumentRoot*. En el código anterior este directorio está bajo `/var/www`, debe crear el nuevo directorio con el comando `mkdir` coincidiendo el nombre con la directiva *DocumentRoot* de código 3. Para el ejemplo mostrado sería `mkdir /var/www/minombre.tai`.

T13.2.- Cree un archivo `index.html` con el editor `nano` en el nuevo directorio creado en al paso anterior que contenga código HTML que muestre su nombre. Si no conoce HTML puede usar cualquier ejemplo de Internet y modificarlo.

T13.3.- Para verificar si la configuración es correcta ejecute el comando `apache2ctl configtest`, si no se muestra error puede reiniciar el servicio con `systemctl restart apache2`. Ahora, navegue a http://www.minombre.tai y http://minombre.tai para comprobar que ver su nombre.

T13.4.- Descargue desde Internet una plantilla HTML para sustituir la página que creó, puede descargarla de alguno de estos enlaces: https://templated.co, http://www.minimalistic-design.com ,

https://foundation.zurb.com/templates.html, etc. Compruebe que se muestra correctamente la plantilla en http://www.minombre.tai.

T13.5.- Navegue a http://servidor1.minombre.tai y verá otra página diferente ¿Donde está situada esta página? ¿Cual es el archivo de configuración que controla este dominio?

El último ejercicio consistirá en realizar la suplantación de una página WEB de la universidad combinando la modificación de los DNS de en la máquina *Servidor2* con el servidor WEB multidominio preparado en *Servidor1*. El objetivo será la plataforma de enseñanza virtual *ev.us.es*.

Tarea 14.- En el servidor de nombres del *Servidor2* cree una nueva zona para *ev.us.es* del mismo modo que se hizo en la Tarea 9.-. Debe definir en esta zona la resolución para www.ev.us.es y ev.us.es, ambas apuntando a la dirección IP del *Servidor1*.

T14.1.- Compruebe si los nuevos dominios se resuelven correctamente desde la máquina *Gateway* usando los comandos `host` y `ping`.

T14.2.- Cree en la máquina *Servidor1* una nueva configuración para estos dos dominios del mismo modo que se hizo en la Tarea 13.-. La página a servir está en el fichero *ev.zip* suministrado con el material del laboratorio. Debe descomprimirlo en una nueva carpeta dentro de `/var/www` (por ejemplo `/var/www/ev`) y configurar correctamente apache para que sirva esta página sólo para estos dos dominios.

T14.3.- Navegue desde la máquina *gateway* a http://ev.us.es y compruebe el resultado.

5. Ejemplos de inseguridad en servicios Web

A continuación se propone la realización de dos ejercicios opcionales relacionados con la seguridad de los servidores Web y de los Navegadores. El primero consiste en realizar la instalación de un WebShell en el servidor Apache. El segundo conseguir realizar la suplantación de un sitio Web a pesar de tener SSL.

Tarea 15.- Opcional-3d: Añada el soporte del lenguaje PHP al servidor Web Apache instalando el paquete `libapache2-mod-php7.0`.

T15.1.- Busque en GitHub algún *WebShell* escrito en PHP. Siga las instrucciones para que el WebShell quede empaquetado cono un único fichero PHP con el nombre `lista-notas.php`.

T15.2.- Añada dicho fichero a su servidor en en la siguiente dirección http://192.168.20.X/lista-notas.php y compruebe el nivel de acceso que tiene a su servidor.

Tarea 16.- Opcional-3e: Añada soporte SSL para el sitio *ev.us.es* en su servidor Apache utilizando como certificados los ficheros suministrados `ev.us.es.crt` y `ev.us.es.pem`.

T16.1.- Navegue desde el ordenador gateway a https://ev.us.es y observe el error de seguridad que aparece, pero no añada una excepción para entrar.

T16.2.- El problema que presenta el certificado SSL ha sido usado es que no se reconoce la autoridad certificadora que lo ha firmado. Para evitar este problema utilice el certificado de autoridad `ca-tai.crt` y añádalo como autoridad de confianza en la configuración de Firefox.

T16.3.- Vuelva a navegar a https://ev.us.es.

T16.4.- Repita el proceso con Firefox en el equipo anfitrión. Para que el equipo del laboratorio

acceda a la versión suplantada de https://ev.us.es. edite el fichero /etc/hosts para introducir una entrada que apunte el dominio *ev.us.es* a la dirección IP pública de su máquina virtual.

6. Recomendaciones y Cuestiones

C1: Si el servidor FTP no inicia correctamente puede deberse a no tener correctamente establecido el nombre de máquina en el fichero /etc/hosts.

C2: Para activar y probar el cifrado con TLS con *proftpd* considere lo siguiente:

- Editar el fichero proftpd.conf y descomentar la inclusión de la configuración de ejemplo en el fichero tls.conf
- Editar el fichero tls.conf y configurar las directivas: TLSEngine, TLSRSACertificateFile y TLSRSACertificateKeyFile.
- Forzar el reinicio con `systemctl stop proftpd stop` y `systemctl start proftpd`. A veces el comando `systemctl restart` no opera correctamente por algún motivo desconocido.

C3: Para ver los errores ocurridos en el servidor de nombres BIND9 se debe acceder a la bitácora del sistema *syslog*, por ejemplo use el comando `less /var/log/syslog` y pulse SHIFT+F para ver en tiempo real los mensajes.

C4: Para comprobar los accesos que se realizan para el servidor WEB apache2 se deben ver los archivos de bitácora /var/log/apache2/access.log y /var/log/apache2/error.log. Es recomendable tener un terminal extra abierto con el comando `tail -f /var/log/apache2/*` ejecutándose.