SERVICIOS TELEMÁTICOS

3º de GII – Práctica final – Junio/Julio 2019/2020

1 Descripción

La práctica final a desarrollar consiste en la configuración y puesta en marcha de un conjunto de servicios telemáticos, descritos en los apartados siguientes, sobre el escenario de red que se muestra a continuación:

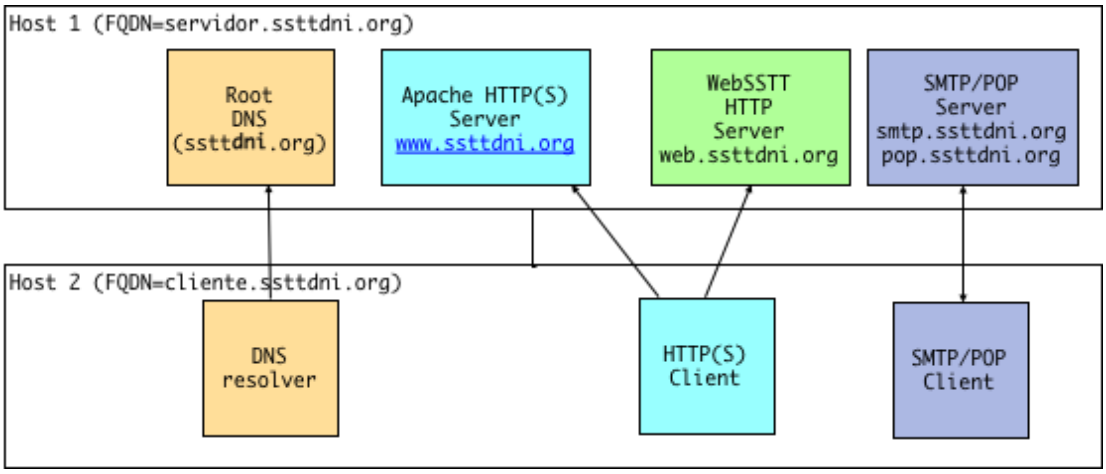

Figura 1. Escenario objetivo para SSTT

Este escenario cuenta con un equipo (*servidor.sstt**dni**.org*) en el que residen los servidores principales de los distintos servicios, y con otro equipo (*cliente.sstt**dni**.org*) donde residen las aplicaciones cliente. IMPORTANTE: ***dni*** indica los últimos 4 dígitos del DNI de la persona que entrega la práctica. Por ejemplo, si el DNI de la persona es 55550000 el dominio será **sstt0000.org**

2 Funcionalidad obligatoria

2.1 Programación Web-SSTT HTTP Server:

Desplegar un servicio HTTP basado en la práctica de programación descrita en la sesión de prácticas 1 (Web-SSTT). Se deberá crear una entrada *web.sstt**dni**.org* en el DNS, y definir una configuración mínima para establecer una página inicial de prueba, que contenga al menos una imagen .gif o .jpg de *más de 8KB de datos*.

Funcionalidad **obligatoria**:

- Tratar la petición HTTP con el método GET básica, que devolverá un fichero HTML con un formulario FORM HTML. El formulario contiene un atributo *method* (*method="post")* para que el navegador realice la petición POST HTTP básica desde un navegador Firefox. **IMPORTANTE**: La plantilla del formulario se proporcionará con la

plantilla del servidor en C. El formulario pedirá un correo electrónico. Al recibir la información del formulario en la petición POST, el servidor comprobará si es el correo del estudiante correo y si lo es, devolverá una página HTML informando que el correo es correcto. Si no fuera el correo del estudiante, la página informará que el correo es erróneo.

- Implementar **mecanismo de persistencia** HTTP. El servicio deberá mantener una conexión abierta durante un tiempo determinado (a elegir por el alumno) y, en el caso de no recibir peticiones durante ese periodo de tiempo, se terminará la conexión. (Nota: recordad las cabeceras Connection y Keep-Alive)
- El fichero HTML también hará referencia, al menos, a una imagen .gif o .jpg. La imagen deberá ser mayor de 8 Kbytes.
- Durante el lanzamiento del servidor, éste debe recibir como parámetro el puerto en el que ha de lanzarse el servicio.
- Verificación de que la petición HTTP es válida. Se debe verificar que la petición y sus cabeceras ha sido definidas de acuerdo con la especificación de HTTP. Además, las cabeceras que se deben incluir son: Host, Server, Content-Type, Content-Length, Date y Connection.

Para verificar la instalación se utilizará un cliente HTTP en *cliente.sstt**dni**.org*, y se consultará la URL: *http://web.sstt**dni**.org*, procediéndose a consultar la página *index.html*.

2.2 Desplegar servicio DNS

Desplegar un servidor DNS raíz. El DNS raíz en *servidor.sstt**dni**.org* deberá gestionar un único dominio de nivel principal. Este dominio se llamará sstt**dni**.org (donde, recuerda, **dni** son los últimos 4 dígitos del DNI de la persona que entrega la práctica). Para verificar el correcto funcionamiento se lanzará el resolver del DNS en *cliente.sstt**dni**.org* y se solicitará la resolución de diferentes nombres de equipo que estén gestionados en el servidor DNS (*cliente.ssttdni.org*, *servidor.ssttdni.org, www.ssttdni.org, web.ssttdni.org, smtp.ssttdni.org, pop.ssttdni.org, etc.*). Esta configuración de nombres y dominios se utilizará en los siguientes apartados de la práctica.

El servicio DNS **deberá (obligatorio)** hacer un reenvío a los servidores DNS de la UMU en el caso de que no sepa realizar una resolución.

Se deberá describir y configurar correctamente el registro MX para el soporte del servicio de correo electrónico.

2.3 Desplegar servicio SMTP/POP

Desplegar un servicio SMTP/POP en *servidor.sstt**dni**.org*, configurando para ello el dominio de correo *ssttdni.org* en el DNS, crear dos usuarios de correo en dicho servidor SMTP: *nombre1_**dni**@sstt**dni**.org* y nombre2_dni@ssttdni.org, y crear una entrada en el DNS para el servidor de correo SMTP (*smtp.sstt**dni**.org*) y otra para el servidor POP (*pop.sstt**dni**.org*).

Para verificar la instalación, se utilizará un cliente POP/SMTP en *cliente.sstt**dni**.org*, que se configurará para leer el correo mediante POP desde

*pop.sstt**dni**.org* y enviar correo mediante SMTP a *smtp.sstt**dni**.org*, entre los usuarios previamente definidos.

Se deberá analizar la relación entre el servicio SMTP y el DNS a través del registro MX. **Indica** si es necesario o no su uso en la práctica y **por qué**.

2.4 Desplegar servicios HTTP/HTTPS

Desplegar un servicio Apache HTTP/HTTPS en *servidor.sstt**dni**.org*, creando una entrada *www.sstt**dni**.org* en el DNS, y dotándolo de la configuración suficiente para establecer una página inicial de prueba y alguna página adicional enlazada. Este servidor HTTP deberá recibir peticiones en el puerto estándar HTTP (puerto 80) y en el puerto estándar para HTTPS (443).

En el servicio HTTP se pedirá el login y password del cliente antes de devolver el contenido.

En el servicio HTTPS se utilizará autenticación de cliente basada en certificados X.509.

Para verificar la instalación se utilizará un cliente HTTP/HTTPS en *cliente.sstt**dni**.org*, y se consultarán las siguientes URLs: *http://www.sstt**dni**.org* y *https://www.sstt**dni**.org*, con las páginas de prueba.

El certificado X.509 de servidor deberá contener en el DN el nombre DNS del servicio web (i.e. www.sstt**dni**.org) y no deberán salir "warnings" de seguridad durante el acceso.

El certificado X.509 de cliente deberá contener en el DN el nombre (sin apellidos) y DNI de la persona que entrega la práctica.

2.5 IPsec

La conexión entre cliente.sstt**dni**.org y servidor.sstt**dni**.org se deberá proteger mediante una asociación de seguridad IPsec modo túnel entre ambos equipos. Se utilizará IKEv2 para el establecimiento de la IPsec SA y la autenticación de las partes se realizará mediante certificados de identidad (se pueden reutilizar los creados en el apartado anterior). Este túnel sólo autenticará (no cifrará) el tráfico entre los dos equipos, obligatoriamente mediante la cabecera AH.

Se deberán establecer los valores criptográficos y las políticas de seguridad correspondientes.

2.6 Otras mejoras (Opcionales)

Se aceptarán y valorarán otro tipo de mejoras adicionales que los/las alumnos/as puedan proponer de forma individualizada previo acuerdo con los profesores de la asignatura. Ejemplo de mejoras:

- Instalar FTP (**máx. 0,5 puntos**).
- Instalar y configurar el servicio DHCP (**máx. 0,5 puntos**).

- Desplegar un servidor DNS secundario del primario que gestiona el dominio “sstt**dni**.org” (**máx. 0,25 puntos**).
- Desplegar un dominio de resolución inversa (**máx. 0,25 puntos**).
- Crear un subdominio ssttdni.org e instalar un DNS para el mismo (**máx. 0,5 puntos**).
- Instalar y configurar IMAP como servidor de correo entrante (**máx. 0,5 puntos**).
- Gestión básica de cookies en el servidor Web-SSTT HTTP. Se enviará una cookie con un contador de accesos al servidor de modo que al décimo acceso se denegará el acceso al contenido. El formato será **cookie_counter**=N, para N={1, 2, 3, 4,…}. El valor de la cookie variará para cada petición del usuario al servidor. Esta cookie expirará a los 2 minutos de su creación (Pista: cabecera Max-Age). (**máx: 1 punto**).
- Añadir a la conexión persistente un límite por número de peticiones y no sólo por tiempo de la conexión TCP activa (**máx. 0,5**).
- Utilizar un analizador sintáctico para procesar las peticiones que llegan del cliente web (**máx. 0,75**).
- Mejorar y proteger los mecanismos de autenticación para el correo electrónico (**máx. 0,25 puntos**).
- Entregar el apartado 2.1 el día 22/03/2020 **(1,5 puntos**).

3 Requisitos

El escenario a diseñar y configurar se desplegará sobre los PCs del laboratorio 2.7 y 2.3. **Se permite el uso de portátiles** en las sesiones de prácticas.

4 Entrega

Entrega anticipada del código C del servidor web: se podrá realizar una entrega anticipada de la práctica correspondiente a la programación del servidor HTTP (2.1). La fecha de entrega será el **22/3/2020**, a través de la tarea correspondiente que se habilitará en AulaVirtual. Esta entrega anticipada supondrá, si está correcta, hasta +**1,5 puntos en la parte de mejoras de la práctica.** Se deberá incluir tanto el código fuente como la documentación asociada. El/La alumno/a que no entregue esta parte en dicha fecha podrá entregarla en junio/julio 2020, pero no obtendrá esta puntuación extra. Si realiza la entrega anticipada pero no presenta el resto de los apartados en junio 2020, en la convocatoria de julio 2020 y febrero 2021 deberá entregar toda la práctica y no se mantendrán el +1,5 extra.

Entrega final: Se realizará una entrega final que corresponderá a los apartados (2.1-2.5). El estudiante publicará todo el material en la tarea correspondiente que se abrirá para la entrega de las prácticas en AulaVirtual. NOTA: En la convocatoria de junio 2020 esta entrega final llevará documentada las partes 2.1-2.5, al igual que en la convocatoria de julio 2020 y febrero 2021, se entregará un único documento con todo (2.1-2.5). La entrega final se realizará durante la semana siguiente a la finalización de las clases (17/5/2020) a través de una tarea que se dejará abierta.

Tanto en la entrega anticipada como en la final se debe incluir **un único** archivo (.pcap) que contenga las trazas capturadas con Wireshark para todos los servicios que se esperan en esa entrega.

No habrá entrevistas de prácticas, salvo que los profesores consideren lo contrario para casos excepcionales.

El material publicado por cada alumno/a se encontrará dentro de un archivo comprimido ***"DNI_Practica_SSTT_1920.zip"*** y contendrá la configuración de los servicios y la documentación. **NO incluir archivos binarios ni librerías.** La documentación deberá incluir los siguientes elementos:

Documentación de la entrega anticipada:

- Descripción de la implementación del servicio Web-SSTT HTTP.
- Una traza representativa del protocolo HTTP implementado, así como una explicación de ésta con los aspectos más relevantes que demuestren el correcto funcionamiento del programa.
- Problemas encontrados en el proceso del desarrollo del escenario.

Documentación de la práctica final:

- Introducción.
- Descripción del escenario desarrollado y versiones de software.
- Descripción de las configuraciones, destacando las opciones de configuración más relevantes.
- Descripción de la implementación del servicio Web-SSTT HTTP.
- Trazas representativas de los distintos protocolos empleados en el escenario, así como una explicación de éstas. En concreto:
    - Una traza que muestre el intercambio DNS y el acceso al web cuando se accede a http://www.sstt**dni**.org.
    - Una traza que muestre el intercambio DNS y el acceso al web seguro https://www.sstt**dni**.org.
    - Una traza que muestre los intercambios DNS, SMTP y POP.
    - Una traza que demuestre el uso de IKE e IPsec. Esta traza debe mostrar paquetes IP protegidos mediante AH de modo que pueda verse el tráfico HTTP, SMTP y POP de los ejemplos anteriores.
- Problemas encontrados en el proceso del desarrollo del escenario.
- Número de horas aproximadas empleadas en cada apartado (2.1-2.5) y en la documentación.
- Conclusiones y valoración personal del trabajo realizado.

Importante:

- Todas las secciones anteriores son **obligatorias**. Si alguna no se presenta o no funciona, la práctica estará suspensa.
- **Las faltas de ortografía implicarán reducción de la nota final de las prácticas, o incluso se podría suspender en casos graves**.
- **NO** se permiten las entregas fuera de plazo.
- No cumplir estas condiciones implica no superar las prácticas.

5 Evaluación

La evaluación de la práctica la realizarán los profesores de la asignatura a través de:

a) Corrección de la documentación presentada por el/la alumno/a.
b) Verificación del funcionamiento de cada uno de los apartados 2.1 a 2.5.

Estas verificaciones se realizarán durante las propias sesiones de laboratorio o en horario de tutorías, donde el profesor constatará, para cada alumno/a, si el trabajo que requiere cada uno de los apartados anteriores (2.1-2.5) está correctamente ejecutado o no (simplemente se anotará **SÍ** o **NO**). El estudiante informará al profesor cuándo quiere hacer la verificación.

Si un estudiante tiene algún NO en alguno de los apartados 2.1-2.5, podrá hacer uso de las horas de tutorías para realizar la verificación, y que se le anote un SÍ en ese apartado.

Es requisito obligatorio para aprobar la parte práctica que todos los apartados estén verificados correctamente (con un SÍ).

La ponderación de cada uno de los aspectos que influirán en la nota final será la siguiente:

- Funcionalidad obligatoria (SÍ en cada apartado) y documentación → 80%.
- Mejoras opcionales → 20%.

Es necesario aprobar la parte práctica para superar la asignatura. La nota mínima para aprobar es de **5 puntos** y supone un **40%** de la nota final de la asignatura.