SERVICIOS TELEMÁTICOS

3º de GII – Práctica final – 2024/2025

1 Descripción

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

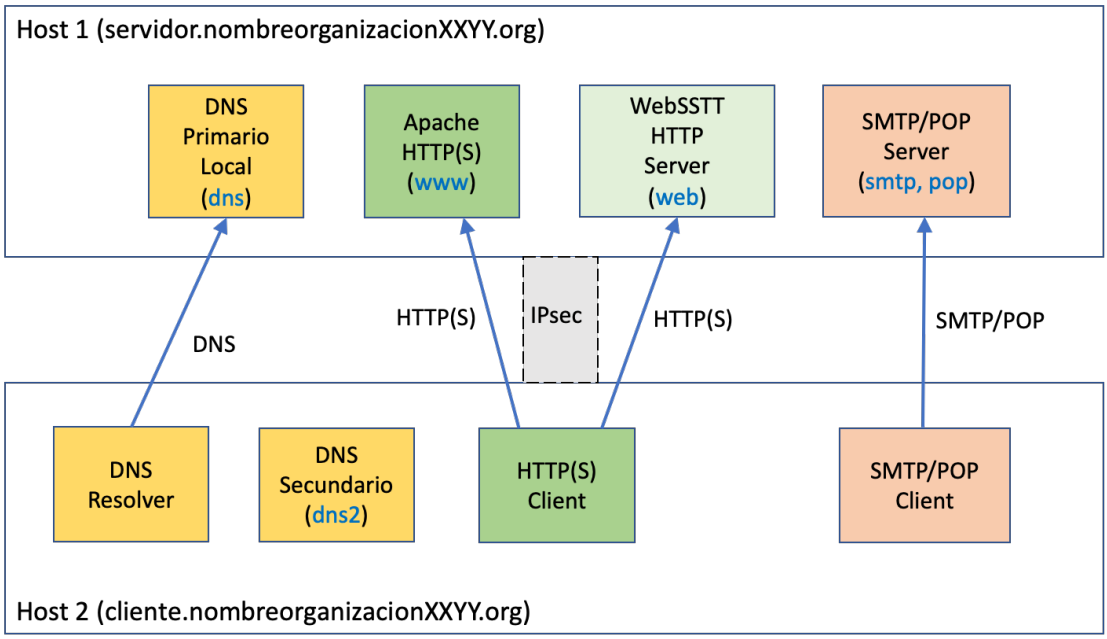

Figura 1. Escenario objetivo para SSTT

2 Escenario

Sobre la topología de red descrita en la Figura 1 los estudiantes deben diseñar un escenario lo más realista posible, donde el despliegue de los servicios tenga coherencia y permita ver un uso adecuado de éstos.

Este escenario debe incluir un nombre de dominio para la organización establecida por los estudiantes en formato "nombreorganizaciónXXYY.org" (por ejemplo abogadosdemurciaXX.com, universidaddemurciaXXYY.es, etc.), definición de los usuarios que harán uso de los servicios, y su identificación (por ejemplo alicia@abogadosdemurciaXXYY.com).

XXYY hace referencia a los dos últimos dígitos del DNI de los estudiantes. Por ejemplo, si el DNI de uno de los miembros es 55550001 y del otro miembro es 55550002 el dominio será **nombreorganización0102.org.**

La elección del escenario a desplegar queda a decisión de los estudiantes y se podrá consultar con los profesores la adecuación de éste a la asignatura.

Este escenario cuenta, al menos, con un equipo (*servidor.nombreorganizaciónXXYY.org*) en el que residen los servidores principales de los distintos servicios, y con otro equipo (*cliente.nombreorganizaciónXXYY.org*) donde residen las aplicaciones cliente.

Se permite el uso de varios equipos servidores para repartir el despliegue de los distintos servicios que se verán en la práctica.

3 Funcionalidad obligatoria

3.1 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.nombreorganizaciónXXYY.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***. Es necesario:

- Gestión básica del método GET en peticiones HTTP request que provienen del cliente y su correspondiente respuesta.
- Gestionar una petición HTTP con el método POST básica de un formulario que el servidor devolverá al cliente en la página index.html. El formulario contiene un atributo *method* (*method="post")* para que el navegador realice la petición POST HTTP básica desde un navegador Firefox. 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 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.
- 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 intento de acceso se denegará el acceso al contenido. El formato será **cookie_counter_XXYY**=N, para N={1, 2, 3, 4,…}. En este caso, XXYY se interpreta como en el nombre de la organización. El valor de la cookie variará solo para cada petición del usuario al recurso index.html del servidor, no para cada recurso. Esta cookie expirará a los 2 minutos de su creación (Pista: cabecera Max-Age).
- Implementar un **mecanismo de persistencia** HTTP. El servicio deberá mantener una conexión abierta durante un tiempo determinado (suma = X+X+Y+Y+10) 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).
- 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 han sido definidas de acuerdo con la especificación de HTTP.

- Verificar que en la petición se ha incluido la cabecera Host.
- Las cabeceras que se tienen que incluir en la respuesta son:
    - Server
    - Content-Type
    - Content-Length
    - Date
    - Connection
    - Keep-Alive
    - Set-Cookie (cuando sea necesario)

- **La cabecera Server deberá indicar el nombre completo del servidor del grupo. Por ejemplo: Server: web.nombreorganizacion0102.org**

Para verificar la instalación se utilizará un cliente HTTP (p.ej Firefox de la máquina virtual que actúa de cliente) en *cliente.nombreorganización**XXYY**.org*, y se consultará la URL: *http://web.nombreorganización**XX**YY*.org, procediéndose a consultar la página *index.html*.

3.2 Desplegar servicio DNS

Desplegar un servidor DNS local primario para gestionar los nombres de los distintos equipos desplegados dentro de la organización. El DNS local en el servidor deberá gestionar un único dominio de nivel principal. Este dominio se llamará nombreorganizaciónXXYY.org (siguiendo el mismo formato anterior).

Para verificar el correcto funcionamiento se lanzará el resolver del DNS en el equipo cliente y se solicitará la resolución de diferentes nombres de equipo que estén gestionados en el servidor DNS:

- *cliente.nombreorganizaciónXXYY.org*
- *servidor.nombreorganizaciónXXYY.org*
- *www.nombreorganizaciónXXYY.org*
- *web.nombreorganizaciónXXYY.org*
- *smtp.nombreorganizaciónXXYY.org*
- *pop.nombreorganizaciónXXYY.org*

Esta configuración de nombres y dominios se utilizará en los siguientes apartados de la práctica.

Se deberá probar el servicio DNS **realizando alguna consulta a un dominio diferente (e.g. www.um.es)** para observar la consulta del servidor DNS configurado a los servidores DNS raíces en el caso de que no sepa realizar una resolución.

Se deberá desplegar, además, un **servidor DNS local secundario** que se actualice periódicamente con la información recibida del primario.

Se deberá describir **mediante un caso de uso,** y configurar correctamente, el registro MX para el soporte del servicio de correo electrónico.

3.3 Desplegar servicio SMTP/POP

Desplegar un servicio SMTP/POP en el equipo servidor y crear dos cuentas de usuario de correo en dicho servidor SMTP:

- *nombre1_**XX**@nombreorganizaciónXXYY.org*
- *nombre2_**YY**@nombreorganizaciónXXYY.org*

Crear, como se ha descrito en el apartado anterior, una entrada en el DNS para el servidor de correo SMTP (*smtp.nombreorganizaciónXXYY.org*) y otra para el servidor POP (*pop.nombreorganizaciónXXYY.org*).

Para verificar la instalación, se utilizará un cliente POP/SMTP en el equipo cliente, que se configurará para leer el correo mediante POP desde *pop.nombreorganizaciónXXYY.org* y enviar correo mediante SMTP a *smtp.nombreorganizaciónXXYY.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.

3.4 Desplegar servicios HTTP/HTTPS

Desplegar un servicio Apache HTTP/HTTPS en el equipo servidor, creando una entrada *www.nombreorganizaciónXXYY.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 y HTTPS se pedirá el login y password del cliente antes de devolver el contenido. Se deberá crear una cuenta de cliente para cada uno de los miembros del grupo.

En el servicio HTTPS se utilizará autenticación de servidor basada en certificados X.509. **No se realizará autenticación** de cliente HTTPS basada en certificados, como se ha indicado anteriormente, el control de acceso por parte del servidor se realizará por un sistema de login y password.

Para verificar la instalación se utilizará un cliente HTTP/HTTPS en el equipo cliente, y se consultarán las siguientes URLs: *http://www.nombreorganizaciónXXYY.org* y *https://www.nombreorganizaciónXXYY.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.nombreorganizaciónXXYY.org) y **no deberán salir "warnings" de seguridad durante el acceso**.

3.5 IPsec

La conexión entre un equipo cliente y un equipo servidor se deberá proteger mediante una asociación de seguridad IPsec en modo transporte 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. Uno de los certificados será el de servidor del apartado anterior y otro se generará completamente nuevo y debe contener en el DN el nombre (sin apellidos) y los DNIs de las personas que entregan la práctica. Esta asociación de seguridad IPsec se establecerá mediante la cabecera ESP con cifrado nulo (sin cifrado) e integridad.

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

3.6 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 y configurar FTP (**máx. 0,5 puntos**).
- Instalar y configurar el servicio DHCP (**máx. 0,5 puntos**).
- Desplegar un dominio de resolución inversa (**máx. 0,25 puntos**).
- Crear un subdominio para nombreorganizaciónXXYY.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**).
- Utilizar un analizador sintáctico para procesar las peticiones que llegan del cliente web (**máx. 0,25**).
- Mejorar y proteger los mecanismos de autenticación para el correo electrónico (**máx. 0,5 puntos**).
- Realizar la autenticación de cliente con certificados en HTTPS (**máx. 0,5 puntos**)

4 Requisitos

El escenario para diseñar y configurar se desplegará en los equipos personales (RECOMENDABLE) o en los equipos del laboratorio. Se proporcionará video explicativo sobre el despliegue, así como el entorno de trabajo virtualizado.

5 Entrega

Entregas anticipadas:

- Código Python del servidor web (V1): se podrá realizar una entrega anticipada de la práctica correspondiente a la programación del servidor HTTP (2.1). La fecha de entrega será el **9/03/2025**, a través de la tarea correspondiente que se habilitará en AulaVirtual. Esta entrega anticipada supondrá, si está correcta, hasta **+2 puntos en la parte de mejoras de la práctica.** Se deberá incluir el código fuente, traza (fichero .pcap) de la traza del funcionamiento y debe verificarse antes de la entrega. Los estudiantes que no entreguen esta parte en dicha fecha podrán entregarla en junio o julio 2025 pero no obtendrán esta puntuación extra. Si realizan la entrega anticipada pero no presentan el resto

de los apartados en junio 2025, en la convocatoria de julio 2025 deberán entregar toda la práctica y se perderá el +2 extra.

- Correo electrónico y DNS (V2): se podrá realizar una entrega anticipada de la práctica correspondiente a las partes de correo electrónico y DNS. La fecha de entrega será el **6/04/2025**, a través de la tarea correspondiente que se habilitará en AulaVirtual. Esta entrega anticipada supondrá, si está correcta, hasta +**1 punto en la parte de mejoras de la práctica.** Debe verificarse antes de la entrega. Los estudiantes que no entreguen esta parte en dicha fecha podrán entregarla en junio/julio 2025, pero no obtendrán esta puntuación extra. Si realizan la entrega anticipada pero no presentan el resto de los apartados en junio 2025, en la convocatoria de julio 2025 deberán entregar toda la práctica y NO se mantendrá el +1 extra.

La entrega final de la documentación de las partes 3.1 a 3.5 se realizará el **11/05/2025** a través de una tarea que se dejará abierta. Aquí se entregará además los vídeos pendientes de verificaciones. Tanto en las entrega anticipadas como en la final se debe **(obligatorio)** incluir **un único** archivo (.pcap) que contenga las trazas capturadas con Wireshark para TODOS los servicios que se esperan en esa entrega (incluido el servicio HTTP desarrollado en Python).

El profesorado se reserva el derecho a realizar entrevistas de prácticas si lo considera necesario. Por ejemplo, si el estudiante realiza conductas de las que pueda inferirse que pretende valerse de conductas, medios o instrumentos fraudulentos, incluida la indebida atribución de identidad o autoría, se le podrá suspender. En su caso, podrá ser objeto de sanción previa apertura de expediente disciplinario.

El material publicado por cada grupo de prácticas:

- Se encontrará dentro de un archivo comprimido ***"DNI1_DNI2_****Practica_SSTT_2425.zip"*.
- Contendrá la configuración de los servicios y la documentación. **NO incluir archivos binarios ni librerías, sólo los ficheros que el estudiante haya modificado.**
- La extensión máxima del documento completo será de **40 páginas**.
- La documentación deberá incluir los siguientes elementos:

Documentación de la práctica final:

- Introducción.
- Descripción del escenario desarrollado, justificación de la organización elegida y versiones de software.
- Descripción de las configuraciones de los servicios desplegados, destacando las opciones de configuración más relevantes. Se mostrará cada fichero de configuración editado junto con las opciones de configuración modificadas y su explicación correspondiente.

- Descripción de la implementación del servicio Web-SSTT HTTP. Se deben describir las partes principales del código: cómo se han implementado el mecanismo de persistencia, cómo se ha implementado la gestión de cookies, gestión de errores HTTP, etc.
- Captura de la parte de la trazas representativas de los distintos protocolos empleados en el escenario, así **como una explicación de éstas**. En concreto:
    - Una imagen de la traza que muestre el intercambio DNS y el acceso al web cuando se accede a http://www.nombreorganizaciónXXYY.org y su explicación.
    - Una imagen de la traza que muestre el intercambio DNS y el acceso al web seguro https://www.nombreorganizaciónXXYY.org y su explicación.
    - Una imagen de la traza que muestre los intercambios DNS, SMTP y POP y su explicación.
    - Una imagen de la traza que demuestre el uso de IKE e IPsec y su explicación. Esta traza debe mostrar paquetes IP protegidos mediante IPsec 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 por el grupo de prácticas en cada apartado (3.1-3.5) y en la documentación. **Para este apartado se recomienda el uso de la herramienta de gestión de trabajo autónomo que aparece en la herramienta Tareas de AV.**
- 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.
- El informe debe estar correctamente formateado, incluyendo índice de contenidos, números de página, títulos de secciones, texto justificado, títulos de las figuras, etc,
- No cumplir estas condiciones implica no superar las prácticas.

6 Evaluación

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

a) Corrección de la documentación presentada por el grupo de prácticas según Rúbrica de evaluación (ver a continuación).
b) Verificación del funcionamiento de los apartados 3.1 a 3.3.

Las verificaciones se harán mediante la entrega de videos explicativos, o en su defecto en el aula o tutorías, donde el profesor constatará, para cada estudiante, si el trabajo que requiere cada apartado anterior (3.1-3.3) está bien ejecutado o no. Los estudiantes informarán al profesor cuándo quieren hacer la verificación.

Para la realización de estos vídeos se dejarán las instrucciones a seguir por parte de los estudiantes.

En los vídeos deben aparecer y participar de modo proporcional todos los miembros del grupo.

La nota de la práctica será individual, no por grupo. Es decir, dos estudiantes del mismo grupo pueden obtener diferentes notas de prácticas.

Es requisito obligatorio para aprobar la parte práctica que todos los apartados estén verificados correctamente según la plantilla propuesta.

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 → 70%.
- Superar las verificaciones de forma adelantada (marzo y abril) o mejoras opcionales → 30%.

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.

7 Rúbrica para la documentación de la parte obligatoria:

TABLA 1. RÚBRICAS				
Criterio	**Peso**	**Sobresaliente (2)**	**Alcanzado (1)**	**Insuficiente (0)**
1. Corrección de la documentación presentada	15%	El documento tiene una estructura clara, incluye todos los contenidos solicitados, contiene figuras, es claro y carece de faltas ortográficas y gramaticales. Un excesivo número de faltas ortográficas y gramaticales puede conllevar la suspensión completa de la práctica	El documento está estructurado, aunque carece de ciertos aspectos formales. La mayor parte de los contenidos solicitados está presente y carece de faltas ortográficas y gramaticales.	El documento carece de estructura y no está redactado correctamente.
2.Programación Servicio HTTP	20%	El programa funciona correctamente. La documentación sobre la funcionalidad básica implementada y sobre la gestión de errores es detallada. Las partes más relevantes del código están documentadas en detalle. El análisis de trazas es detallado.	El programa funciona correctamente. La documentación sobre la funcionalidad básica implementada y sobre la gestión de errores es correcta. Las partes más relevantes del código están documentadas. El análisis de trazas es correcto.	Los alumnos no responden en la documentación con soltura a las preguntas formuladas.
3. Apache HTTP	10%	La configuración de Apache es correcta. La documentación tanto de configuraciones como de trazas es detallada.	La configuración necesaria para que el servicio Apache funcione según las especificaciones indicadas es correcta y la descripción es adecuada. El análisis de trazas es correcto.	La configuración no es correcta y/o no está bien documentada. El análisis de trazas no es correcto y/o no está bien documentado.
4. Correo electrónico	15%	La configuración de los servicios SMTP y POP es correcta y detallada. En análisis de trazas es detallado	La configuración de los servicios SMTP y POP es correcta y la descripción es adecuada. El análisis de trazas es correcto	La configuración no es correcta y/o no está bien documentada. El análisis de trazas no es correcto y/o no está bien documentado.
5. DNS	15%	La configuración del servicio DNS es correcta. Todos los ficheros de configuración necesarios para el correcto funcionamiento están comentados en detalle. El análisis de trazas es detallado	La configuración del servicio DNS es correcta. Todos los ficheros de configuración necesarios para el correcto funcionamiento están documentados de forma adecuada. El análisis de trazas es correcto.	La configuración no es correcta y/o no está bien documentada. El análisis de trazas no es correcto y/o no está bien documentado.

6. HTTPS	15%	La configuración del servicio Apache para HTTPS es correcta y está documentado de modo detallado. Se muestra el contenido del certificado creados y se describe. El análisis de trazas es detallado.	La configuración del servicio Apache para HTTPS es correcta y está documentado de modo correcto. Se muestra el contenido del certificado creado y se describe. El análisis de trazas es correcto.	La configuración no es correcta y/o no está bien documentada. El análisis de trazas no es correcto y/o no está bien documentado.
7. IPsec	10%	La configuración necesaria para IPsec es correcta y está documentada de modo detallado. El análisis de trazas es detallado.	La configuración necesaria para IPsec es correcta y está documentada de modo adecuado. El análisis de trazas es correcto	La configuración no es correcta y/o no está bien documentada. El análisis de trazas no es correcto y/o no está bien documentado.