ACTIVIDAD - IMPLEMENTACIÓN DE SERVICIOS DE RED SEGUROS
TECNOLOGÍA EN GESTIÓN DE REDES DE DATOS
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL
SENA MEDELLÍN, REGIONAL ANTIOQUIA.

IMPLEMENTACIÓN DE SERVICIOS DE RED SEGUROS CON CERTIFICADOS SSL/TLS.

INTRODUCCIÓN.

Decimos que una conexión es segura cuando está cifrada. Es muy simple, ¿verdad? ¿Pero de dónde proceden los certificados y cuál es la diferencia entre SSL y TLS? Además, ¿qué relación tienen los certificados digitales con la seguridad?

Los certificados SSL/TLS funcionan al vincular digitalmente una clave criptográfica a la información de identificación de una empresa. Esto les permite cifrar las transferencias de datos de tal manera que no puedan ser descifrados por terceros.

SSL/TLS funciona al tener tanto una clave privada como una pública, así como claves de sesión para cada sesión segura única. Cuando un visitante escribe una dirección con seguridad SSL en su navegador web o navega a través de una página segura, el navegador y el servidor web se conectan. Durante la conexión inicial, las claves pública y privada se utilizarán para crear una clave de sesión, que luego se utilizará para cifrar y descifrar los datos que se transfieren. Esta clave de sesión seguirá siendo válida por un tiempo limitado y solo se utilizará para esa sesión en particular.

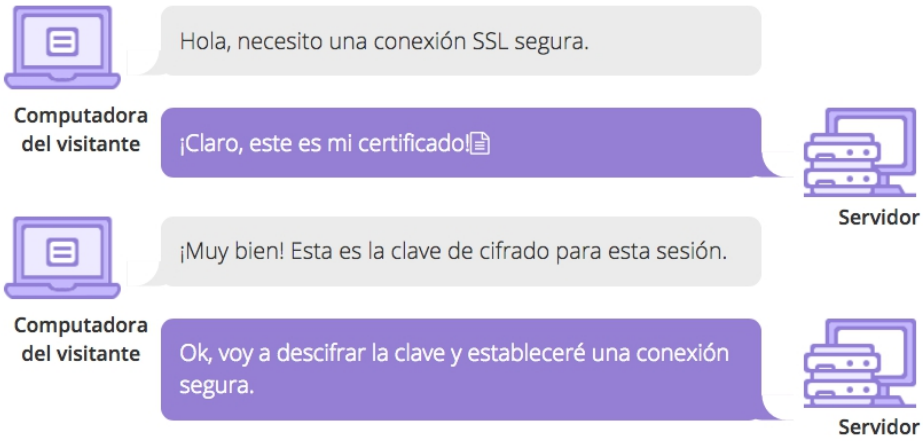


Figura 1. Conexión SSL/TLS. Imagen tomada de https://www.hostinger.es/tutoriales/ssl-tls-https/

El primer protocolo creado para este propósito fue SSL (siglas en inglés para “capa de puertos seguros”). Hubo varias versiones del protocolo SSL y todas ellas tuvieron problemas de seguridad. Por ello apareció una nueva versión con el nombre TLS (siglas en inglés para “seguridad de la capa de transporte”), actualmente en uso. Sin embargo, aunque se le haya cambiado el nombre, sigue conociéndose comúnmente con las iniciales antiguas.

Para cifrar los datos, los sitios requieren un certificado, también llamado firma digital, que confirma que el mecanismo de cifrado es de confianza y cumple con el protocolo. Además de las letras S en HTTPS, otra forma de identificar un sitio seguro es con el candado verde (o escudo en algunos navegadores) y la frase Es seguro o el nombre de la empresa en la barra de direcciones del navegador.

Con esta actividad el aprendiz tendrá la capacidad de implementar un sistema de Infraestructura de Clave Pública para generar y firmar certificados SSL/TLS y asegurar los diferentes servicios de red solicitados.

OBJETIVOS:

- *Instalar los paquetes y roles necesarios para la configuración de una Autoridad de Certificación.*
- *Crear certificados SSL/TLS y auto-firmarlos para asegurar servicios de red.*
- *Asegurar los diferentes servicios para proporcionar seguridad en las conexiones cliente/servidor usando certificados SSL/TLS.*
- *Usar los clientes correspondientes (HTTPS, FTPES, SMTPS, IMAPS, POP3S, etc) para verificar el correcto funcionamiento de los servicios asegurados.*

Responda las siguientes preguntas:

1. ¿En qué consiste una Infraestructura de Clave Pública (PKI) y para qué sirve? ¿ Cuáles son los componentes del PKI? ¿Qué es una CA? Definir los tipos de CA.

2. ¿Qué es SSL? ¿Qué es TLS? ¿Tipos de certificados SSL/TLS?

3. ¿Cómo funcionan los certificados SSL/TLS?

4. ¿En qué ocasiones y por qué se debería tener SSL/TLS?

5. ¿Cómo se relaciona SSL/TLS con HTTPS?

6. Describa cuales son las principales ventajas y desventajas del uso de conexiones encriptadas mediante SSL/TLS.

7. ¿Qué papel juega la criptografía y el criptoanálisis en la seguridad informática mediante certificados SSL/TLS?.

8. ¿Qué es una firma digital? Con sus propias palabras explique como funciona una firma digital.

9. Investigue cuales son los puertos de conexión segura para los principales servicios de red (al menos 15).

10. Realice un mapa conceptual de los principales problemas que se resuelven con el uso de certificados SSL/TLS para cifrar las conexiones de red.

CASO DE ESTUDIO:

La empresa ABC, después de un Análisis de Vulnerabilidades y de Riesgos, ha decidido poner en marcha un Plan de seguridad de la información para mitigar ciertos problemas de confidencialidad que se han venido presentando. El primer paso del plan de seguridad de la información consiste en el aseguramiento de los principales servicios de red mediante el uso de certificados SSL/TLS. A continuación se presenta la topología de trabajo y los requerimientos de la misma en cuanto al aseguramiento y encriptado de las conexiones cliente/servidor:

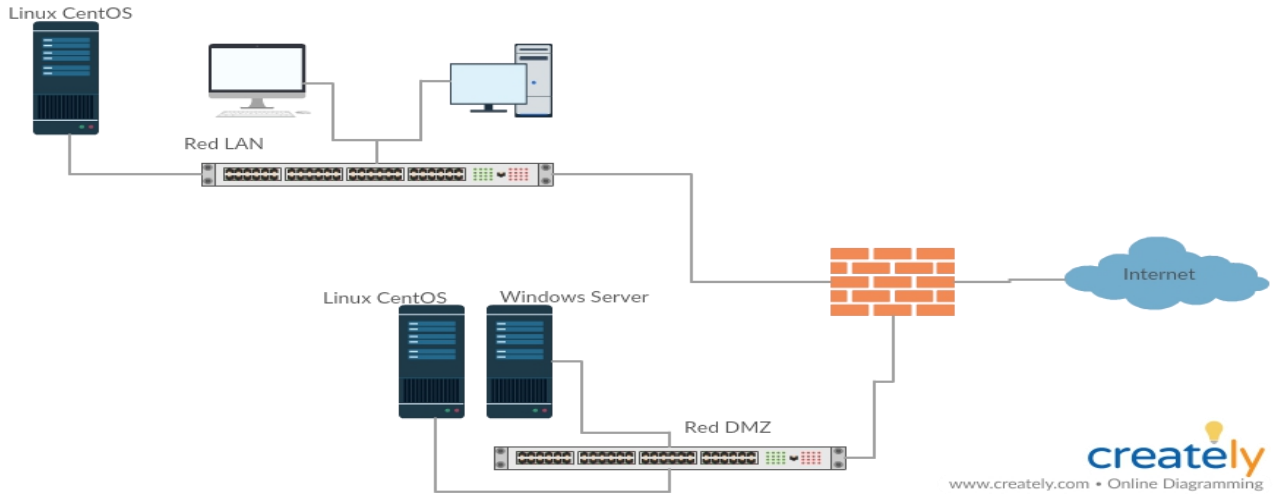


Figura 2. Topología de trabajo.

CONFIGURACIONES:

0. Asigne los nombres de host (*hostname*) a sus servidores de la siguiente forma:

- **Windows Server**: wnserver
- **Enterprise Linux**: lnserver

1. **Red LAN**:

Este segmento de red posee una máquina servidor con el sistema operativo Linux CentOS 7. Los servicios ofrecidos por este servidor son:

- HTTP con el portal web y aplicativo de nómina de la empresa.
- FTP para subir y bajar archivos de forma local desde los equipos de la LAN.

Se requiere asegurar los servicios HTTP y FTP prestados por este servidor mediante el uso de certificados SSL/TLS

2. **Red DMZ**:

Este segmento de red posee dos servidores que salen a Internet. Uno de ellos con Windows Server 2012 R2 y el otro con Linux CentOS 7.

Los servicios prestados por el servidor con Windows Server son:

- Servidor HTTP con la página Web de servicios de la empresa.
- Servidor DNS local de la empresa.

Los servicios prestados por el servidor con Linux CentOS son:

- Servidor SMTP para correo entrante y saliente.
- Servidor IMAP y POP3 para recepción de correo
- Servidor DNS secundario, para fines de redundancia.

Se requiere asegurar los servicios prestados por estos servidores mediante el uso de certificados SSL/TLS.

INSTRUCCIONES:

3. La Infraestructura de Clave Pública -**PKI**- se implementará en una plataforma **Microsoft Windows Server**, instalando el/los roles correspondientes para configurar la CA; generar los certificados autofirmados y posteriormente asegurar los servicios solicitados.

4. La Infraestructura de Clave Pública -**PKI**- se implementará en una plataforma **GNU Linux**, instalando los paquetes correspondientes para configurar la CA, generar los certificados autofirmados y posteriormente asegurar los servicios solicitados.

EVIDENCIAS A PRESENTAR:

1. Informe del proyecto siguiendo las normas técnicas vigentes de presentación de documentación. Incluir un marco teórico en el que se expliquen todos los conceptos y protocolos usados para la implementación.

Tener en cuenta: *calidad de la redacción (No se admite copiar y pegar), explicación detallada de la INSTALACIÓN y CONFIGURACIÓN de las aplicaciones (Imágenes explicadas detalladamente), resumen de las dificultades encontradas en la implementación y la descripción de la solución hallada y conclusiones que evidencien el proceso de indagación y búsqueda de las soluciones a los problemas planteados.*

2. Máquinas virtuales con las implementaciones configuradas y en funcionamiento.

REFERENCIAS BIBLIOGRÁFICAS:

- https://www.hostinger.es/tutoriales/ssl-tls-https/
- https://latam.kaspersky.com/blog/certificates-are-different/12798/
- https://www.tecnoinver.cl/uso-de-protocolos-seguros-para-la-transferencia-de-datos-en-internet/
- https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_9.0.0/com.ibm.mq.sec.doc/q009910_.htm

- https://www.certsuperior.com/SSLtls.aspx
- https://www.websecurity.symantec.com/es/es/security-topics/what-is-ssl-tls-https
- https://es.wikipedia.org/wiki/Infraestructura_de_clave_pública
- https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-on-centos-8
- https://techexpert.tips/es/iis-es/habilitar-https-en-iis/

	Nombre	Fecha
Autor(es)	Rodrigo Ebrat Carr	3/10/2021
Ajustado por		