Fecha límite para la entrega de la práctica: 27 de octubre de 2024

1. OBJETIVO

En esta práctica se aborda el protocolo HTTPS (*Hypertext Transfer Protocol over Secure Socket Layer*), que es la base del servicio WWW seguro. También se trata la certificación X.509 y las infraestructuras PKI. Cubriremos los siguientes objetivos:

- Descripción de las conexiones HTTPS
- Presentación de la librería OpenSSL
- Configuración del modulo SSL/TLS de Apache. Servidores virtuales.
- Definición de una CA (Autoridad de Certificación) y gestión de certificados
- Autentificación de clientes Web mediante certificados

Usaremos una máquina virtual Linux con distribución Ubuntu para construir la PKI y configurar servidores virtuales HTTPS. Para realizar las pruebas usaremos nuestro propio equipo de usuario, o cualquier otro que cuente con interface gráfico y navegador web.

Nota: en el SO Windows, ubicar los certificados de la práctica de en el repositorio de **USUARIO**.

2. PRÁCTICO

1. Comprobar que la máquina virtual Linux cuenta con fecha y hora válidas. Si no es así, actualizar la fecha/hora del sistema. Puede utilizarse el comando `date -s`, o NTP.
2. Instalar en la VM el servidor Apache y activar el módulo SSL. Iniciar el servidor y comprobar que acepta conexiones HTTPS. Describir las características del certificado que envía el servidor. Justificar las razones de la alerta que nos muestra nuestro navegador.
3. Identificar la ubicación del archivo openssl.cnf. Crear una Autoridad de Certificación propia, con los siguientes parámetros por defecto: CountryName (ES), StateOrProvinceName (Madrid), LocalityName (Alcorcon) y OrganizationName (CA de Pruebas). A continuación, obtendremos las claves pública y privada de la CA (archivo cakey.pem, protegido por frase de paso) y un certificado autofirmado con CN = “CA de Pruebas” (cacert.pem). Por último, obtenemos el listado de certificados revocados (crl.pem) que inicialmente estará vacío.
4. Crear una pareja de claves pública y privada RSA de 2048 bits para nuestro servidor web y un certificado firmado por nuestra CA. El CN (y el nombre alternativo SAN) deberá corresponder con el nombre del servidor (**www.seguro.com**). Configurar Apache para que atienda las peticiones dirigidas al dominio por HTTPS (redirigir también las conexiones HTTP hacia HTTPS). La página de inicio estará en /**proyectos**/**seguro**. Llevar a cabo los pasos necesarios para que nuestro cliente pueda conectar con el servidor vía HTTPS sin que se visualice ningún *warning* (reconociendo la CA y el certificado del servidor).
5. Crear un certificado de cliente a nombre de **Víctor Vera** (CN), del departamento de **Ventas** (OU), firmado por nuestra CA. A continuación, configurar el servidor Apache para que requiera certificados cliente **en la raíz del proyecto** a todas las conexiones HTTPS. Establecer una conexión HTTPS con el navegador y verificar que se requiere el certificado de cliente para el acceso. Instalar el certificado en el navegador y verificar que es posible visualizar la página principal del servidor web.
6. Crear un nuevo certificado a nombre de **Pilar Perez** (CN), del departamento de **Personal** (OU), e instalarlo en el navegador. En el servidor web, crear dos directorios, Ventas y Personal, con una página de inicio en cada uno. Configurar el servidor Apache para que sólo permita el acceso a estos directorios a los miembros de los respectivos departamentos (campo OU), tras la autentificación mediante certificado al entrar en el sitio web.
7. Revocar el certificado del cliente Víctor Vera, y actualizar el archivo de certificados revocados de la CA. Configurar Apache para leer el archivo de revocaciones y comprobar a continuación que el usuario revocado ya no puede acceder vía HTTPS a los contenidos del servidor web.

8. Vamos a configurar un nuevo servidor virtual HTTPS para el dominio **www.midominio.com** (con su propio DocumentRoot, en /proyectos/midominio). Las peticiones podrán hacerse sin incluir el prefijo www, y también tendremos en cuanta que algunos usuarios prefieren usar el nombre de dominio **www.midominio.org** (nuevamente no será necesario incluir el prefijo www). Llevar a cabo la configuración del servidor, que contará con su página de inicio. Comprobar que accedemos al contenido del servidor sin errores ni alertas usando cualquiera de los nombres propuestos.
9. Suponga que ahora se decide usar ambos dominios (**www.midominio.com** y **www.midominio.org**) como dos proyectos independientes (con sus respectivos DocumentRoot y página de inicio). Configurar Apache para atender a ambos dominios. Nota: aunque es posible, en este apartado no usaremos nuevos certificados emitidos por nuestra CA; vamos a **reutilizar el certificado creado para el apartado anterior**.
10. Crear un certificado *wildcard* para ***.gameover.com**. Añadir un nuevo servidor virtual para **pinball.gameover.com**, usando el nuevo certificado. Verificar que es posible acceder a los servicios de pinball.gameover.com y www.gameover.com usando el mismo certificado digital y sin errores.
11. Firmar un documento PDF. Para realizar este apartado será necesario contar con una pareja de claves pública /privada y un certificado personal a nombre del alumno. Si es posible, se realizará con el DNI electrónico (se requiere un lector de *SmartCard*) o con un certificado personal emitido por alguna CA reconocida (por ejemplo, la FNMT). Si no se cuenta con ninguno de estos certificados, también es posible usar un certificado a nuestro nombre emitido por nuestra propia CA (en este último caso, se deberá adjuntar en el envío el certificado raíz de esta CA). El documento PDF puede ser la propia memoria de la práctica, y tendrá la firma visible en la última página del documento.
12. **Partes opcionales**:
    - Crear una nueva PKI que cuente con una autoridad raíz y una autoridad intermedia derivada de esta, que se encargue de emitir los certificados. Emitir un certificado para un servidor web firmado por la autoridad intermedia. Por último, crear un archivo .pem que contenga la cadena de certificación completa (certificado del dominio, autoridad intermedia y autoridad raíz).
    - Con el fin de promover el uso de conexiones HTTPS de forma generalizada, la entidad certificadora **Let's Encrypt** (https://letsencrypt.org/) ofrece desde 2016 certificados gratuitos reconocidos por la mayor parte de los navegadores. Estudiar y documentar el proceso que debe seguirse para la obtención de estos certificados y su renovación periódica (es necesario tener registrado el dominio).
    - Seleccionar alguna herramienta opensource para desplegar y mantener una PKI (OpenXPKI, Dogtag, etc.). Instalar y probar la herramienta elegida.

3. FORMA DE ENTREGA

Una vez finalizada la práctica se entregará una memoria justificativa en formato PDF, que podrá ir firmado digitalmente. La memoria deberá incluir los pasos seguidos para la realización de cada tarea planteada, comandos utilizados y dificultades encontradas. Al menos deberá cubrir las tareas 2 a 11, siendo opcional la propuesta realizada en el apartado 12.

La memoria será ordenada, clara y legible, e irá encabezada con el nombre de los autores. Se deberán evitar los "listados" innecesarios. Si se considera de interés, podrán incorporarse como anexos a la memoria, debidamente reseñados.

El resultado será un documento único en formato PDF denominado practica2-SPD.pdf que se enviará antes de la fecha de cierre a la dirección de correo electrónico teo.rojo@ceu.es.

Se podrá requerir a los autores la defensa de la práctica. Deberá guardarse una copia de la máquina virtual utilizada en el desarrollo, para poder verificar, si fuera necesario, su correcto funcionamiento.