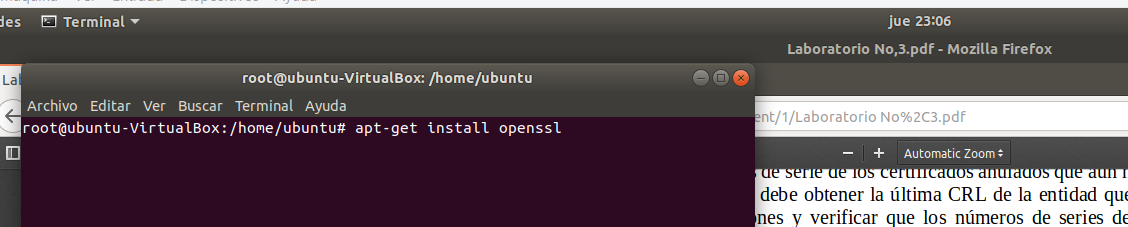
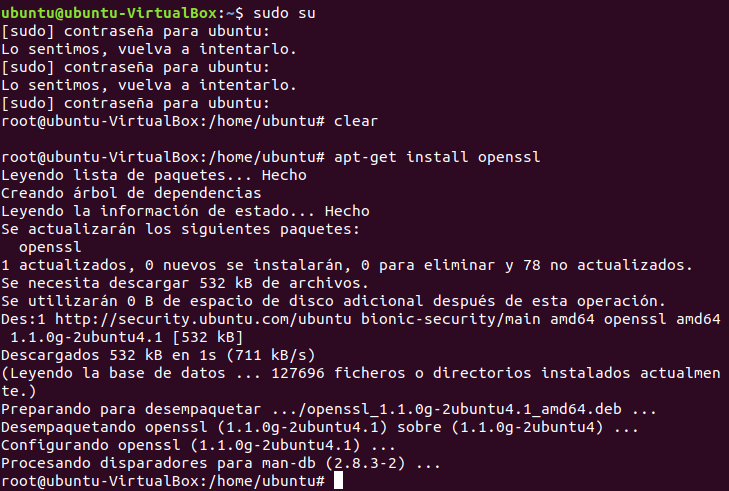
***Laboratorio 3 SSL y SSH***

**SECCIÓN NO. 1 Instalación de OpenSSL y Creación del Certificado SSL para servidor Apache**

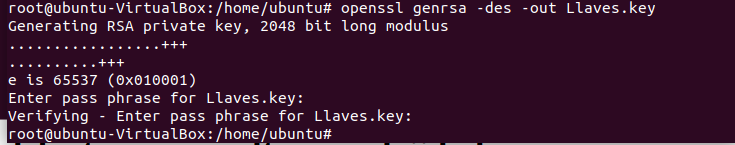
1. Instalación de paquetes openssl.



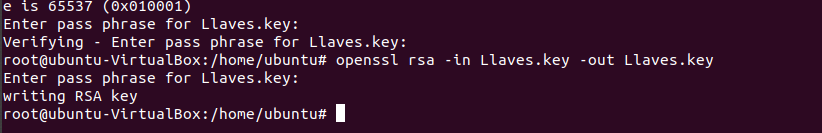
2.Descarga de archivos para el funcionamiento de openssl



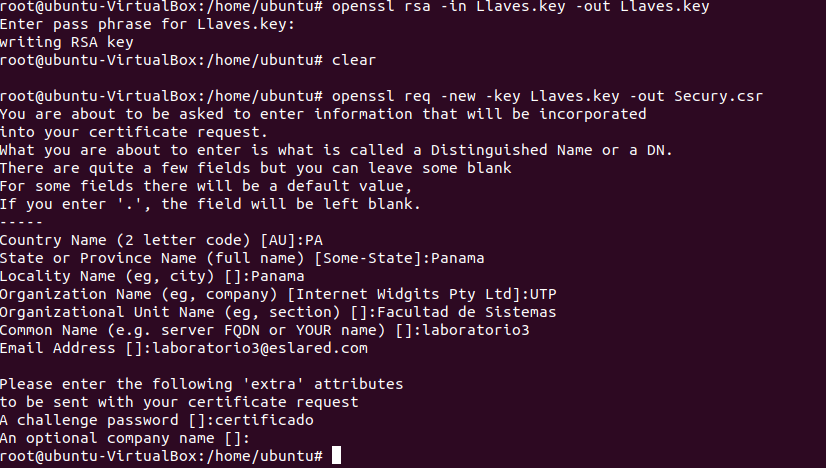
3.Generación de llave RSA.



4.Sustitución de clave del servidor RSA.



5.Crear nombre al servidor Secury y asignar la claver anterior, se llenan datos solicitados de Country, State, Locality, Organizational, Common name, email.

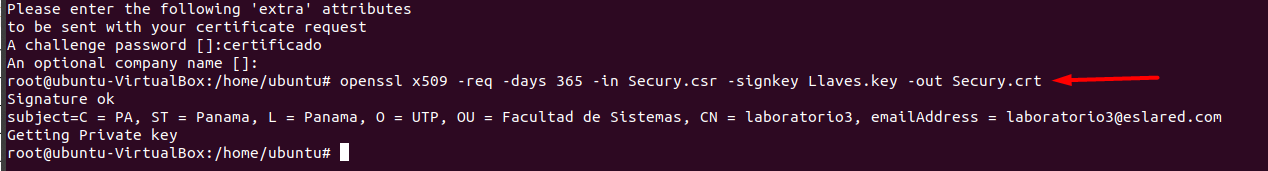


El siguiente comando es:

#openssl x509 –reg –day 365 –in Secury.csr –signkey Llaves.key –out Secury.crt:

Generación de certificado con 365 días de validez

6. Generación de certificado con 365 días de validez



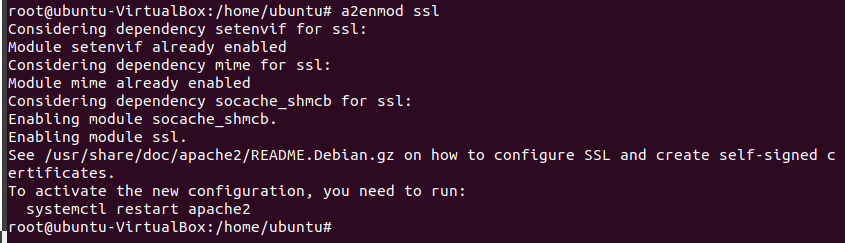
7. Creacion de carpeta ssl dentro del apache2



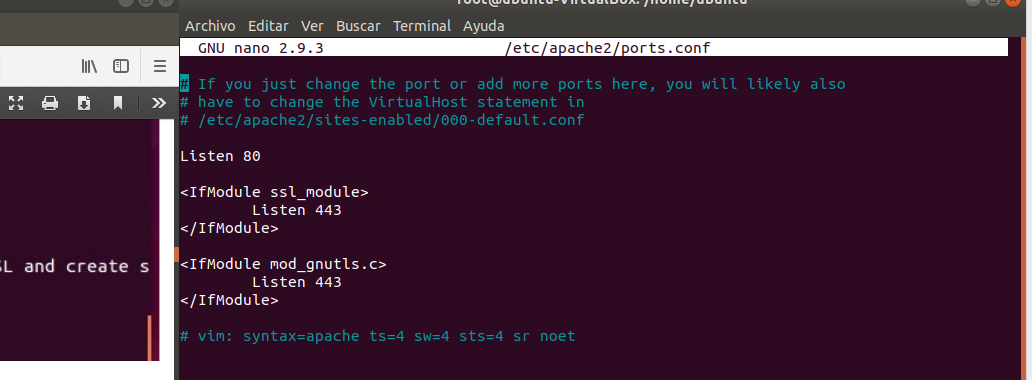
8. Mover las llaves y el Secury a la carpeta ssl anteriormente creada.



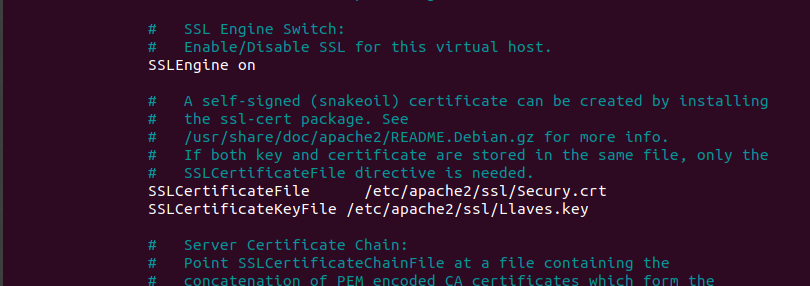
9. Habilitar modulos ssl para apache.



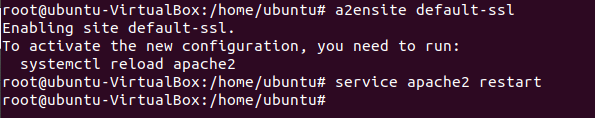
10. Verificación de puertos.



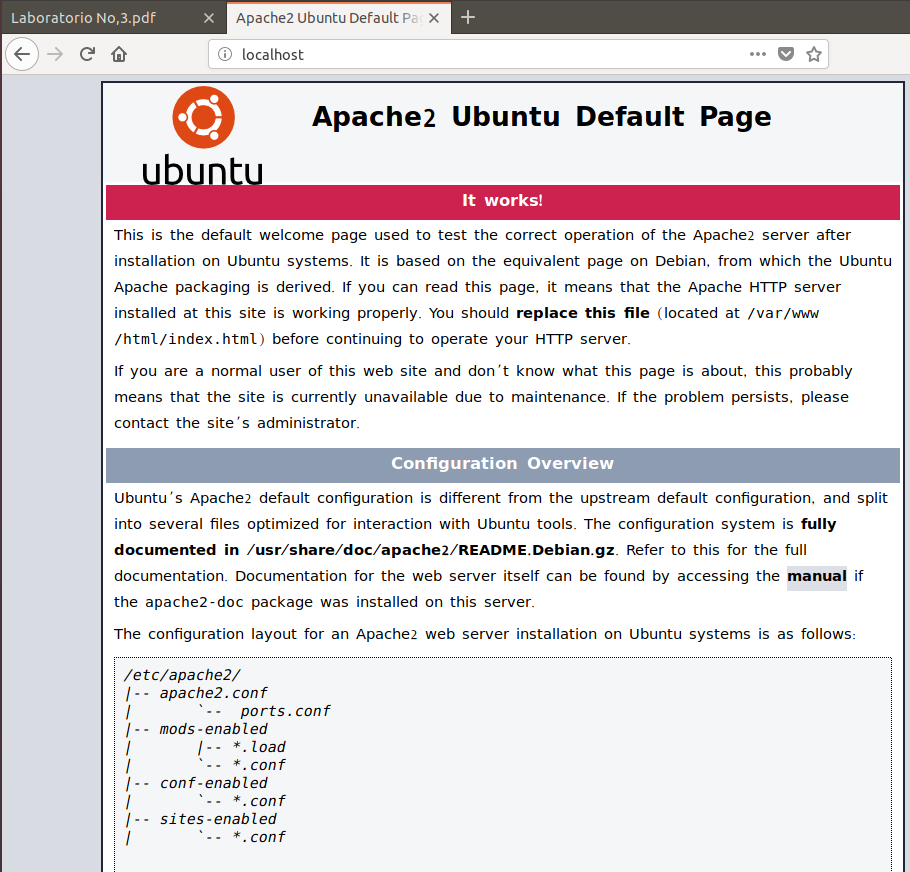
11. Modificación de los archivos SSLCertificateFile y SSLCertificateKeyFile.



12. Habilita la configuración SSL de apache por defecto.

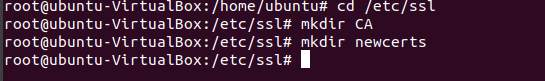


13. Vista de el servidor local de apache.

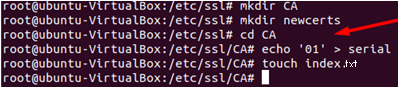


**SECCIÓN NO. 2 Crear Autoridad de Certificación (CA)**

1. Creación de carpetas CA y newcerts



2. Crear dentro del directorio CA el archivo serial con el texto 01 y crear archivo en blanco index.txt



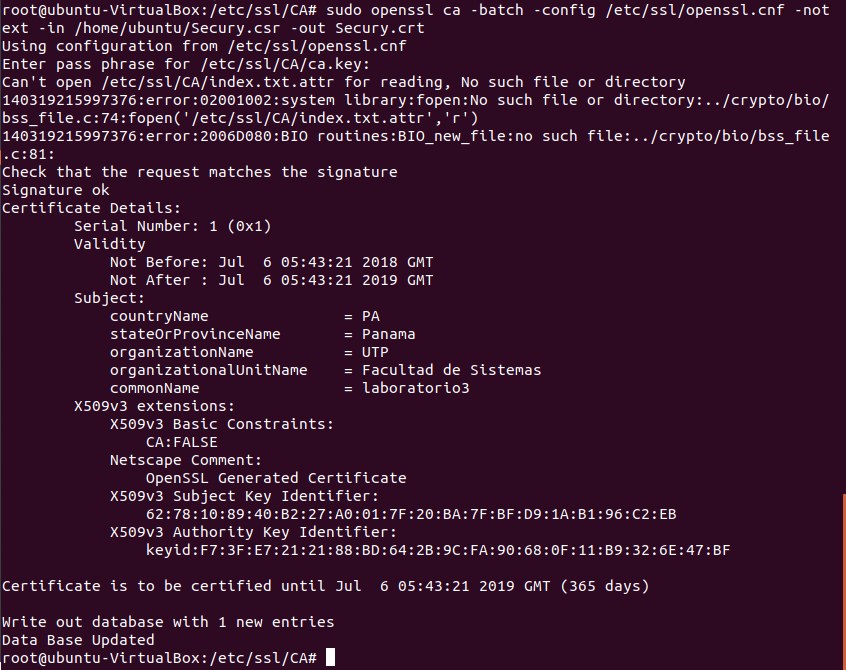
3.Configuracion de openssl.cnf a los solicitados de la guía.



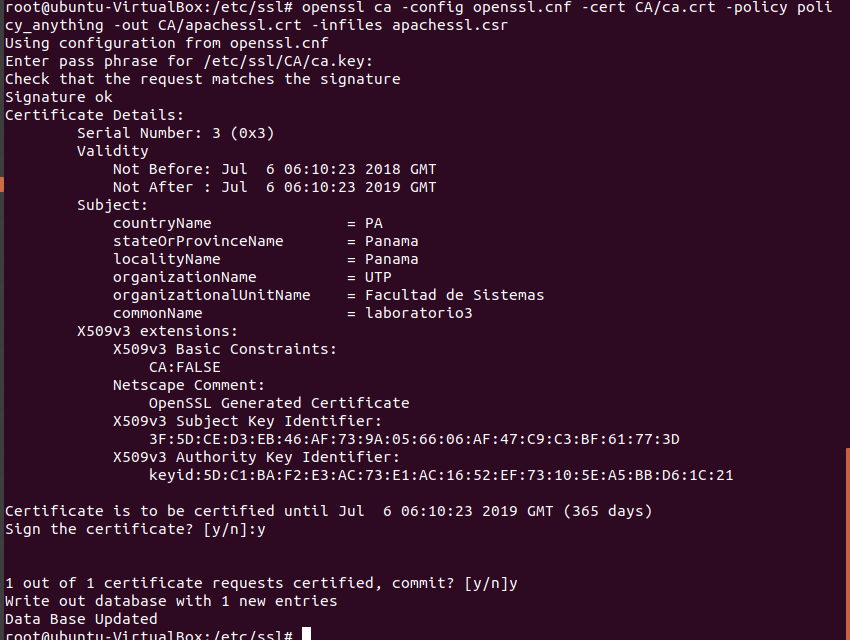
4. Creación del certificado.



5. Firmar con la CA privada el servidor web.



6. firma certificado para generar el servidor.

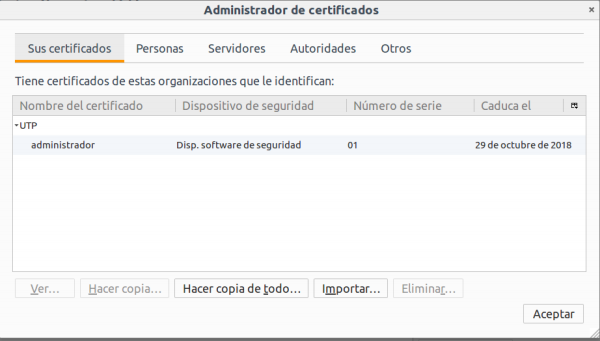


7. Exportación de archivo pkcs12 para las configuraciones de certificado digital del navegardor.



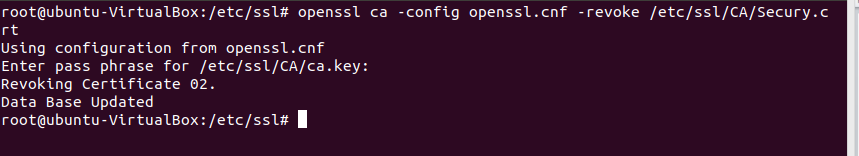


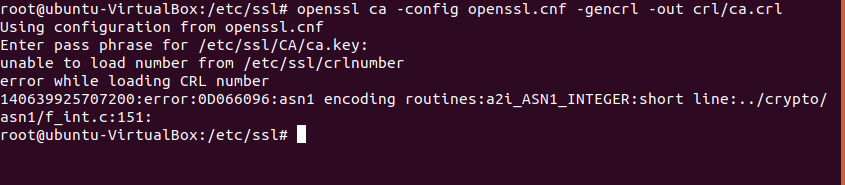
8. Importar certificado creado.



***SECCIÓN NO. 3 Utilización de las Listas de Revocación de Certificados (CRL)***

1. Revocar certificado válido para que deje de funcionar



2. Generar nueva firma digital.

***SECCIÓN NO. 4 Generación de certificados X.509***

**Errores al desarrollar esta sección.**

En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

***Investigue:***

1. ¿En qué consiste el formato pem utilizados en la clave y el certificado de la Autoridad

Certificadora?

***R:*** Este es un formato contenedor que puede incluir sólo el público certificado (como con Apache se instala, y archivos de certificados de CA /etc/ssl/certs), o puede incluir toda una cadena de certificados, incluyendo la clave pública, la clave privada, y de los certificados de root. El nombre de Privacidad de Correo electrónico Mejorada, un error de método para correo electrónico seguro, pero el formato de envase que se utiliza vidas, y es un base64 traducción de la x509 ASN.1 teclas.

2. ¿Cuál es el funcionamiento de las líneas de comando introducidas al shell en el paso 7 de la sección 3?

***R:*** La sección 3 solo tiene dos líneas de comando no hay paso 7.

3. ¿Es posible utilizar un certificado digital generado por una AC implementada en Linux para proveer soporte SSL (utilizando certificados digitales) a un Servidor Web basado en Windows, como por ejemplo IIS? Explique

Se puede ya que crearlo en ubuntu no quiere decir que solo sea para linux, al final son certificados que se instalan en los navegadores de internet como lo es google chrome, firefox, safari, opera.

4. Presentar el procedimiento a seguir para instalar un certificado digital en un servidor Web Microsoft IIS 6.0.

Para instalar el certificado:

1. Abra el Administrador de servicios Internet y expanda el nombre del servidor para que pueda ver los sitios Web.
2. Haga clic derecho en el sitio Web para el que creó la solicitud de certificado y haga clic en Propiedades.
3. Haga clic en la ficha Seguridad de directorios. En Comunicaciones seguras, haga clic en Certificado de servidor. Esto inicia al Asistente para la instalación de certificados. Haga clic en siguiente para continuar.
4. Seleccione procesar la petición pendiente e instalar el certificado y haga clic en siguiente.
5. Escriba la ubicación del certificado que ha descargado en la sección "Emisión y descarga un certificado" y haga clic en siguiente. El asistente mostrará el resumen del certificado. Compruebe que la información es correcta y haga clic en siguiente para continuar.
6. Haga clic en Finalizar para completar el proceso.

5. Investigar 3 razones para indicar que un certificado ya no es válido.

***R:*** Las razones son:

* Caducidad
* Bloqueo de firewall
* Certificados desconocidos.
* Certificados mal generados.

6. Investigue 5 sitios Web de Internet en donde se pueden encontrar Listas de Revocación de Certificados (CRL)

Lista de certificados revocados.

* https://certificacion.cgcom.es/infoacomc/crl

Las listas de revocación de certificados incluyen los números de serie de todos los certificados que han sido revocados. Estas listas se actualizan cada 24 horas y pueden ser consultadas a través de las siguientes URL:

* http://crl3.cgcom.es/crl/eccgcom.crl
* http://crl4.cgcom.es/crl/eccgcom.crl

***ULTIMA PARTE***

1. Con la información y los conocimientos que ha adquirido trate de llenar la tabla siguiente. Marque aquellas casillas que puedan obtenerse con las funciones que se mencionan en cada caso. Tome como ejemplo la primera fila.

