CatarsysLab

Memoria técnica de la implementación de la solución en servidores

Proyecto: ESTUDIO DISEÑO Y REINGENIERÍA DEL SISTEMA DE ATENCIÓN DE DENUNCIAS E INVESTIGACIÓN DE OFICIO (2a VERSIÓN)

Cliente: PROCURADURÍA AMBIENTAL Y DEL ORDENAMIENTO TERRITORIAL DEL D.F.

Índice

1. Implementación de la solución en servidores

A continuación se expone la memoria técnica resultado de la implementación de la solución que comprende el Sistema de Atención de denuncias e Investigación de Oficio en los servidores indicados por la Procuraduría Ambiental y del Ordenamiento territorial del D.F.

1.1 Implementación de archivos – Permisos de usuario

Una vez localizado el archivo comprimido que contiene el paquete que permitirá alojar los servicios XAMPP, se procede a descomprimirlo. Esta descompresión necesita los permisos de algún usuario con perfil de administrador, o en su defecto, ejecutar las instrucciones y/o comandos bajo un ambiente equivalente y seguro; en este caso, se indica mediante el parámetro -s a la instrucción sudo, para lograr este ambiente.

Es importante mencionar que este ambiente o configuración de permisos, es necesario para descomprimir dicho archivo. De otra manera, el intérprete de comandos lanzara un error haciendo referencia a las capacidades insuficientes de la cuenta del usuario en cuestión para llevar a cabo esta operación.

Otra manera de resolver esta situación, seria iniciar sesión con un usuario el cual tiene los permisos suficientes para llevar a cabo esta tarea. Comúnmente identificado con el alias “root”.

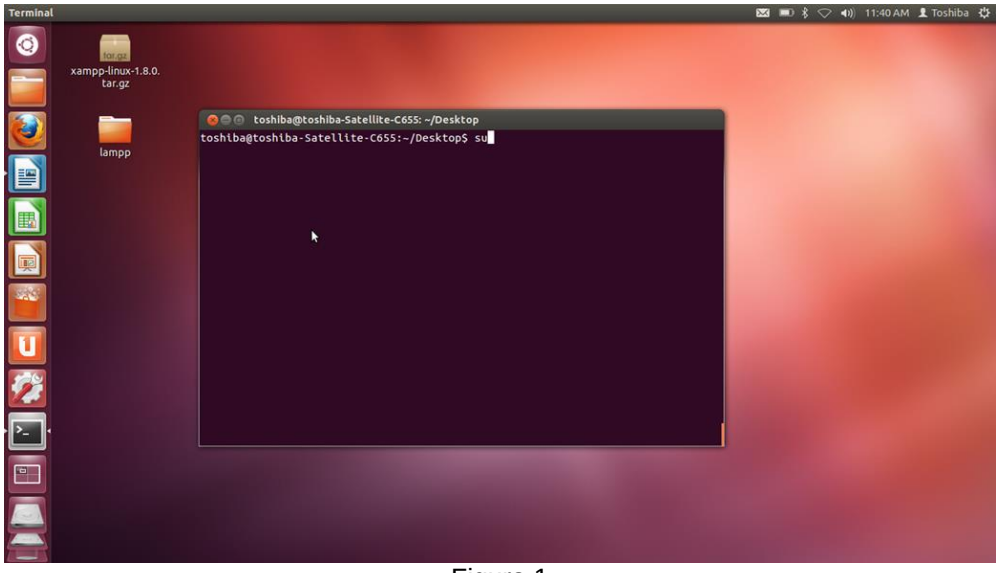

Figura 1
Root en Shell

La Figura 1 muestra la línea de comandos posicionada sobre la carpeta que contiene el archivo comprimido xampp-linux-1.8.0.tar.gz,y, dentro de esa carpeta se ejecuta el comando el cual permite visualizar los usuarios y los respectivos permisos que poseen. ls -l

Las instrucciones que se ejecuten sobre dicha línea de comandos, tendrán efectos sobre la carpeta donde el usuario este posicionado, de esta manera, el archivo a descomprimir debe estar en la carpeta actual. O, también existe la posibilidad de ejecutar la herramienta de descompresión indicando el nombre del archivo junto con su ruta completa.

Se sugiere posicionarse sobre la carpeta superior donde se encuentra el archivo, con el fin de evitar confusiones, además de minimizar los errores al capturar dicha ruta.

Para una explicación más veraz del comando ls, a continuación se muestra su descripción encontrada en el manual que incluye el intérprete de comandos.

NOMBRE
ls - listar el contenido del directorio

SINOPSIS
ls [OPCIÓN] ... [ARCHIVO] ...

DESCRIPCIÓN
Lista de información sobre los archivos del directorio actual (por defecto). Ordenar alfabéticamente las entradas si ninguno de cftuvSUX ni - sort es especificado.

Los argumentos obligatorios para las opciones largas son también obligatorios para las opciones cortas.

-a, - all
no ignore las entradas que empiezan por.

-A, - casi todos
no la lista implícita. y ..

- autor
con-l, imprima el autor de cada archivo.

-b, - escape
impresión de tipo C. escapes para caracteres no gráficos.

- block-size = TAMAÑO
ampliar tamaño por tamaño antes de imprimirlas. Por ejemplo, `- block-size = M 'imprime tamaños en unidades de 1.048.576 bytes. Ver formato TAMAÑO
a continuación.

-B, - ignore-backups
no se muestren las entradas implícitas que terminan en ~

-c con-lt: ordena por, y exposición, ctime (hora de la última modificación de la información de archivo de estado) con-l: muestra ctime y ordenar por nombre de otro modo: Ordenar por ctime más reciente primero.

-C entradas de la lista de columnas

Una vez ubicado dicho archivo, xampp-linux-1.8.0.tar.gz, se prosigue a generar el ambiente pertinente donde se ha de descomprimir el archivo sin incidentes. Esto se hace mediante el comando sudo -s.

El parámetro s indica al intérprete de comandos que la contraseña del usuario no deberá pedirse en próximas ejecuciones de comandos, mientras no se cierre la sesión.

Es importante resaltar este parámetro porque permitirá ahorrar tiempo de respuesta en cuanto a la ejecución de las instrucciones, ya que no será necesario volver a teclear dicha contraseña en repetidas veces.

A continuación se muestra una revisión rápida de los parámetros de esta instrucción , obtenido del manual del interprete de comandos.

NOMBRE
sudo, sudoedit - ejecutar un comando como otro usuario

SINOPSIS
sudo [-D nivel]-h |-K |-k |-V

sudo-v [-AKNS] [-D nivel] [-g nombre de grupo | # gid] [-p prompt] [-u nombre de usuario | # uid]

sudo-l [l] [-AKNS] [-D nivel] [-g nombre de grupo | # gid] [-p prompt] [-U nombre de usuario] [-u nombre de usuario | # uid] [comando]

sudo [-AbEHnPS] [-C fd] [-D nivel] [-g nombre de grupo | # gid] [-p prompt] [-u nombre de usuario | # uid] [VAR = valor] [-i |-s] [comando]

sudoedit [-AnS] [-C fd] [-D nivel] [-g nombre de grupo | # gid] [-p prompt] [-u nombre de usuario | # uid] archivo ...

DESCRIPCIÓN

sudo permite a un usuario le permite ejecutar un comando como superusuario o usuario a otro, como lo especifica la política de seguridad. El real uid y gid efectivo y se ponen a coincidir con los del usuario de destino, tal como se especifica en la base de datos de contraseñas, y es el vector de grupo inicializa a partir de la base de datos del grupo (a no ser que la opción-P se ha especificado).

sudo es compatible con una arquitectura plug-in para las políticas de seguridad y de entrada / salida del registro. Los terceros pueden desarrollar y distribuir su propia política y de E / S de registro módulos para trabajar fichero de tus ajustes con el extremo delantero sudo. La política de seguridad por defecto es sudoers, que es configurada a través del archivo / etc / sudoers, oa través de LDAP.

La política de seguridad determina qué privilegios, en su caso, un usuario tiene que ejecutar sudo. La política puede requerir que los usuarios se autentican a sí mismos con una contraseña u otro mecanismo de autentificación. Si se requiere autenticación, sudo se cerrará si la contraseña del usuario no se introduce dentro de un límite de tiempo configurable. Este límite es una política específica, el tiempo de espera de contraseña por defecto del sistema para los sudoers política de seguridad es ilimitado.

Las políticas de seguridad pueden apoyar el caché de credenciales para permitir al usuario ejecutar sudo de nuevo por un período de tiempo sin necesidad de autenticación. La política sudoers almacena en caché las credenciales durante 15 minutos, a menos que se remplaza en sudoers (5). Al ejecutar sudo con el v-opción, el usuario puede actualizar las credenciales almacenadas en caché sin ejecutar un comando.

Cuando se invoca como sudoedit, la opción-e (que se describe más adelante), se implica.

Las políticas de seguridad pueden registrar los intentos exitosos y fallidos de usar sudo. Si un plugin de E / S se configura, el comando de entrada de corriente y de salida puede estar conectado también.

1.2 Descompresión de archivos de la solución

Una vez ubicado el archivo, y sabiendo que se cuentan con los permisos necesarios para descomprimirlo, se procederá a indicarle a la herramienta de descompresión, mediante parámetros acordes a la ruta donde se encuentra dicho archivo, la ejecución de esta tarea.

Dicha tarea se ejecutara mediante el comando tar, el cual llamara a la herramienta de descompresión. Un vistazo más certero acerca de esta herramienta se puede encontrar en el manual del interprete de comandos. Se anexa un vistazo a esta información, para comprender mejor la forma en que el intérprete de comandos analiza dicha tarea de descompresión; además de que los parámetros opcionales, pueden servir si algún archivo no funcionara bien o se encontrase corrupto.

NOMBRE
tar - La versión de GNU de la utilidad de archivado tar

SINOPSIS
tar [-] A - catenate - concatenar | c - create | d - diff - compare | - delete | r - append | t - list | - test de etiqueta | u - update | x
- extracto - get [opciones] [nombre de ruta ...]

DESCRIPCIÓN
Almacena el archivo descomprimido en la carpeta indicada.

El primer argumento debe ser una función, ya sea uno de los Acdrtux cartas, o uno de los nombres de las funciones de largo. Una función let- ter no necesita tener el prefijo `` -'', y puede ser combinada con otras opciones de una sola letra. A nombre de la función a largo debe tener el prefijo -. Algunas opciones de tomar un parámetro, con la forma de una letra estos deben ser dados como argumentos separados. Con la forma larga, se puede administrar añadiendo = valor de la opción.

CARTAS DE FUNCIONES
Modo de operación principal:

-A, - catenate, - concatenate
adjuntar archivos tar a un archivo

-c, - create
crear un nuevo archivo

-d, - diff - compare
encontrar diferencias entre archivos y sistema de archivos

- eliminar
eliminar del archivo (no en cintas mag!)

-r, - append
anexar archivos al final de un archivo

-t, - list
listar el contenido de un archivo para ejecutar correctamente la herramienta de descompresión/compresión, se deberán incluir como parámetros el nombre del archivo y la ruta donde se alojara dicho resultado de la descompresión.

En este caso, la ruta será bajo la carpeta opt, ya que aquí se encuentran alojadas las aplicaciones mas comunes; además de los servicios.

Analizando el comando que permitira descomprimir:

tar xvfz xampp-linux-1.8.0.tar.gz -C /opt

Podemos notar la llamada a la sentencia tar, la cual espera como parámetros, además de los opcionales, el tratamiento que se le dará a dicho archivo:

x - extract
z - decompress
v - see file name
f - file name

También cabe destacar que se usa la directiva -C para crear las carpetas, o estructura de carpetas donde se descomprime el archivo. Esto con la finalidad de poder continuar dicho proceso sin necesidad de verificar o preguntar al usuario si desea crear la o las carpetas involucradas.

Es importante resaltar, aunque ya se menciono en el punto numero 1, que si el usuario en cuestión no cuenta con los permisos suficientes para ejecutar la descompresión, esta no se llevara a cabo; puesto que la carpeta opt es una carpeta de sistema y por lo tanto tiene restricciones en cuanto a su escritura, lectura o ejecución.

Una vez que se ha ejecutado dicho comando, aparecerá en el intérprete de comandos, el seguimiento del proceso, desplegando el detalle de la

descompresión de cada archivo. Esto es útil ya que además de poder estimar el tiempo de descompresión, el cual en este caso es mínimo para este paquete, se puede revisar este log para conocer los problemas que pudieran existir con dicha tarea.

Los problemas mas comunes de la descompresión, son relacionados a los permisos que se tienen en cuenta para la sesión en la en el interprete de comandos, además de los típicos errores de captura (ya sea la ruta, o el nombre del archivos).

Sea el caso que se manifieste mediante el comportamiento en la descompresión, siempre se podrá ejecutar nuevamente, ya que hasta el momento no se ha iniciado el servidor y no afectaría en dicho levantamiento.

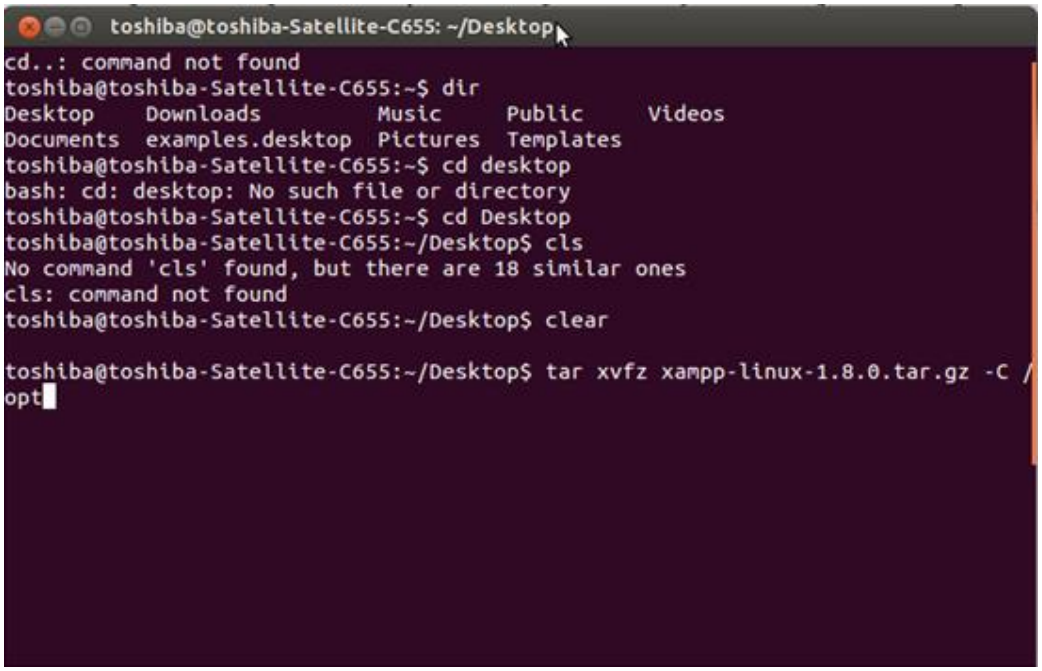

Figura 2
Descompresión

1.3 Inicialización

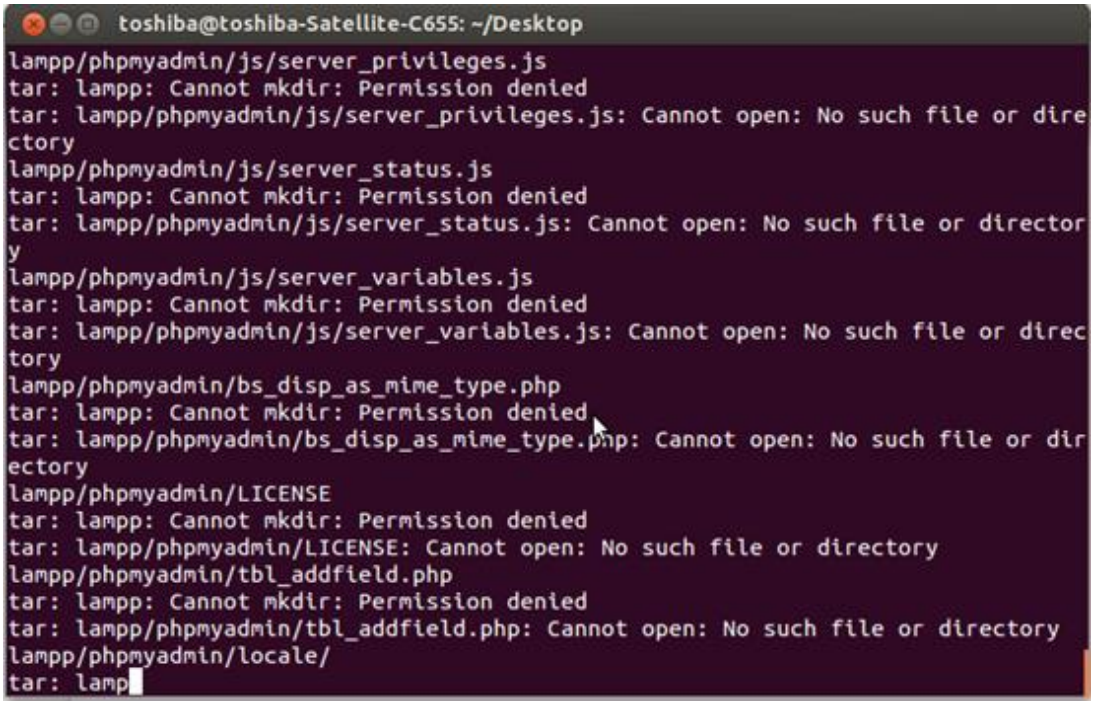

Figura 3
Inicialización

Como se muestra en la Figura 3 anterior, la descompresión se completó satisfactoriamente, lo cual da pie a preparar el ambiente necesario para inciar el servidor XAMPP.

Es importante mencionar los servicios de esta entidad para conocer que se ha instalado:

Apache

El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.12 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue rescrito por completo. Su nombre se debe a que

Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. En inglés, a patchy server (un servidor "parcheado") suena igual que Apache Server.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años. (Estadísticas históricas y de uso diario proporcionadas por Netcraft3).

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

MySQL

MySQL es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.1 MySQL AB —desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual.

Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y los derechos de autor del código están en poder del autor individual, MySQL es patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

Esto es lo que posibilita el esquema de licenciamiento anteriormente mencionado. Además de la venta de licencias privativas, la compañía ofrece soporte y servicios. Para sus operaciones contratan trabajadores alrededor del mundo que colaboran vía Internet.

ProFTPD

ProFTPd es un servidor FTP. Se promociona desde su página web como estable y seguro, cuando se configura correctamente. El servidor ProFTPd se promociona a sí mismo como un "Software servidor FTP altamente configurable con licencia GPL" ("Highly configurable GPL-licensed FTP server software").

Los promotores dicen que ProFTPd está bien documentado, y la mayoría de configuraciones serán muy parecidas a aquellas que aparecen en las configuraciones de ejemplo. ProFTPd usa un único fichero de configuración "/etc/proftpd.conf". El fichero de configuración es muy similar al que tiene Apache. Puede ser fácilmente configurado como múltiples servidores FTP virtuales, y tiene capacidades para ser enjaulado dependiendo del sistema de archivos que haya por debajo. Puede ejecutarse con un demonio propio o como un servicio más de inetd. Es capaz de trabajar sobre IPv6.

Su diseño es modular, lo que permite escribir extensiones como cifrado SSL/TLS, RADIUS, LDAP o SQL como módulos.

Ahora que se tienen identificados los módulos que componen XAMPP, se procede a iniciar dicho servidor. Por iniciar se podría entender el proceso de comenzar a liberar los servicios necesarios para que las aplicaciones puedan ejecutar código. De esta manera, el servidor de base de datos el cual tiene sentido con un lenguaje de servidor que en este caso es PHP, a implementar, pueden comprender que hay un servidor que puede atender sus peticiones.

La petición inicial de un servidor, refiriéndose a su cola es como inicia esta comunicación, pues se verifica si el servidor esta prendido. Esto, por su puesto, tiene su contraparte al detener este servidor. Ya que los procesos son interrumpidos en el caso de PHP y en el caso de MySQL los datos ligados a esos procesos. Reportando una caída de servicio. En este caso, al ejecutar

aplicaciones de XAMPP, se crea un servidor virtual privado, comparado a una instancia; pero con la particularidad de manejar los archivos “en el aire”.

Por lo tanto, es muy posible confundir un error de configuración de cada servicio con una tipica 404 not found.

Rápidamente se accede al intérprete de comandos, nuestro viejo aliado en creación de scripts los cuales pueden barrer estos servidores privados virtuales en búsqueda del problema, lograr terminar ese proceso, e iniciar los servicios nuevamente. La siguiente imagen muestra la ruta donde se encuentra la ejecución del servidor padre XAMPP.

Es importante explicar esto pues en consecuencia, al reiniciar XAMPP se reinician MySQL, Apache(PHP) en conjunto.

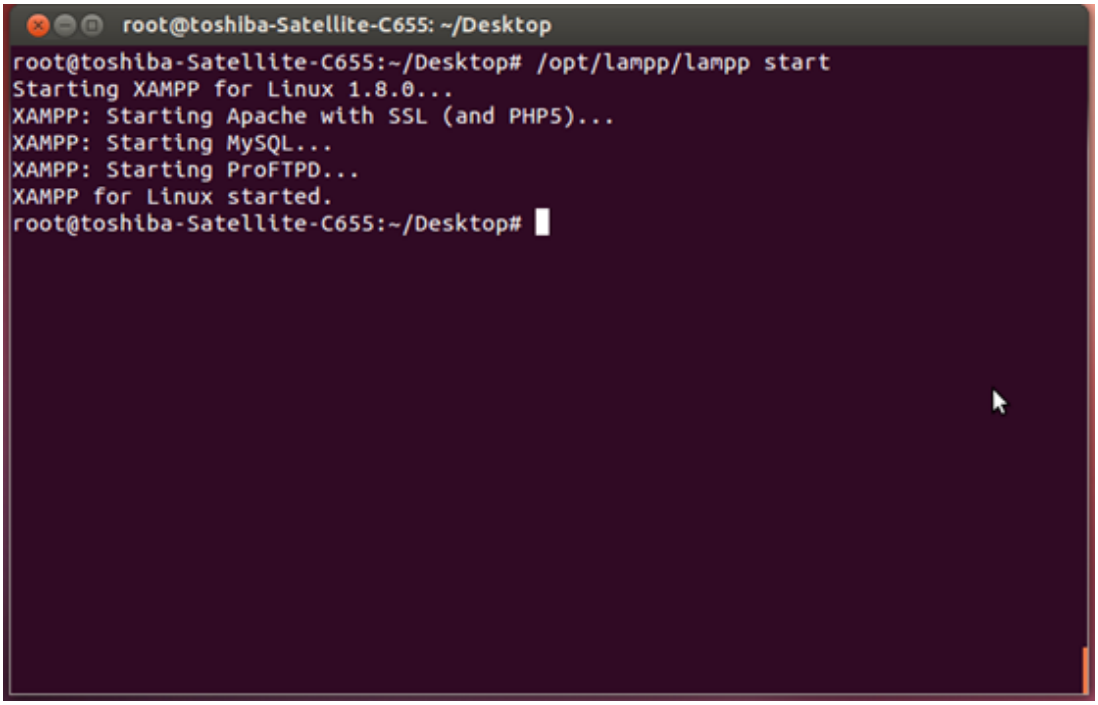

Figura 4
Iniciando el servidor

De esta manera tenemos iniciado por primera vez nuestro servidor XAMPP, lo cual podemos constatar dirigiéndonos a nuestro directorio virtual raíz y explorando el sitio web correspondiente. Se podría decir que si aparece, nos encontramos en una situación ejemplar, de mucho valor y éxito, al poder configurar e instalar XAMPP.

Basta ir a su navegador preferido y teclear en la barra de dirección después de www.

http://localhost/xampp/

Figura 5
Servidor listo

Básicamente, al ver esta ventana, en el idioma que usted prefiera, el servidor está listo.

Para poder agregar un sitio web, es necesario cambiar los permisos.

El servidor estará configurado hasta que estos permisos son los adecuados para poder tener una base de datos y una tecnología de servidor, en este caso PHP mediante Apache pueden funcionar.

1.4 Permisos

En la instalación predeterminada, XAMPP no tiene contraseñas establecidas y no se recomienda para funcionar con esta configuración de XAMPP accesible por otros (por ejemplo, en Internet).

Simplemente escriba el siguiente comando (como root) para iniciar una comprobación de seguridad simple:

/opt/lampp/lampp security

Ahora debería ver el siguiente cuadro de diálogo en la pantalla (la entrada del usuario está resaltado):

LAMPP: Quick security check...
LAMPP: Your LAMPP pages are NOT secured by a password.
LAMPP: Do you want to set a password? [yes] yes (1)
LAMPP: Password: ******
LAMPP: Password (again): ******
LAMPP: Password protection active. Please use 'lampp' as user name!
LAMPP: MySQL is accessable via network.
LAMPP: Normaly that's not recommended. Do you want me to turn it off? [yes] yes
LAMPP: Turned off.
LAMPP: Stopping MySQL...
LAMPP: Starting MySQL...
LAMPP: The MySQL/phpMyAdmin user pma has no password set!!!
LAMPP: Do you want to set a password? [yes] yes
LAMPP: Password: ******
LAMPP: Password (again): ******
LAMPP: Setting new MySQL pma password.
LAMPP: Setting phpMyAdmin's pma password to the new one.
LAMPP: MySQL has no root passwort set!!!
LAMPP: Do you want to set a password? [yes] yes
LAMPP: Write the passworde somewhere down to make sure you won't forget it!!!
LAMPP: Password: ******
LAMPP: Password (again): ******
LAMPP: Setting new MySQL root password.
LAMPP: Setting phpMyAdmin's root password to the new one.
LAMPP: The FTP password is still set to 'lampp'.
LAMPP: Do you want to change the password? [yes] yes
LAMPP: Password: ******
LAMPP: Password (again): ******

LAMPP: Reload ProFTPD...
LAMPP: Done.

Todas estas configuraciones se establecen para su consulta en un archivo llamado httpd.xampp.conf

Es interesante el manejo de estos archivos, pues permiten modificar en tiempo real la configuración del servidor XAMPP, para poder reiniciar rápidamente los servicios y tener un mínimo de porcentaje de servidor caído, inclusive en el sitio web se muestran las estadísticas por día y agrupadas por semana.

Esto es de apreciarse, pues permite conocer el incremento de recursos para poder tomar acciones; de esta manera, si la tendencia es de crecimiento de datos, se puede ir previniendo la instalación de discos, o si el procesamiento no es el esperado en cuanto a performance, se puede ir pensando en aumentar la memoria o cambiar los procesadores.

Estos archivos se encuentran en la ruta /opt/lampp/ext/extra

Hay 2 secciones que se deben existir para poder ver un sitio correctamente, en este caso un sitio ya instalado como phpmyadmin que viene como modulo de XAMPP

Nuestra aplicación está escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando Internet

Actualmente puede crear y eliminar Bases de Datos, crear, eliminar y alterar tablas, borrar, editar y añadir campos, ejecutar cualquier sentencia SQL, administrar claves en campos, administrar privilegios, exportar datos en varios formatos y está disponible en 62 idiomas. Se encuentra disponible bajo la licencia GPL.

Este proyecto se encuentra vigente desde el año 1998, siendo el mejor evaluado en la comunidad de descargas de SourceForge.net como la descarga del mes de diciembre del 2002. Como esta herramienta corre en máquinas con Servidores Webs y Soporte de PHP y MySQL, la tecnología utilizada ha ido variando durante su desarrollo.

Con este proceso se puede confirmar checar si un sitio ya es visible.

Aquí se enlista como quedaría el archivo en las 2 secciones mencionadas:

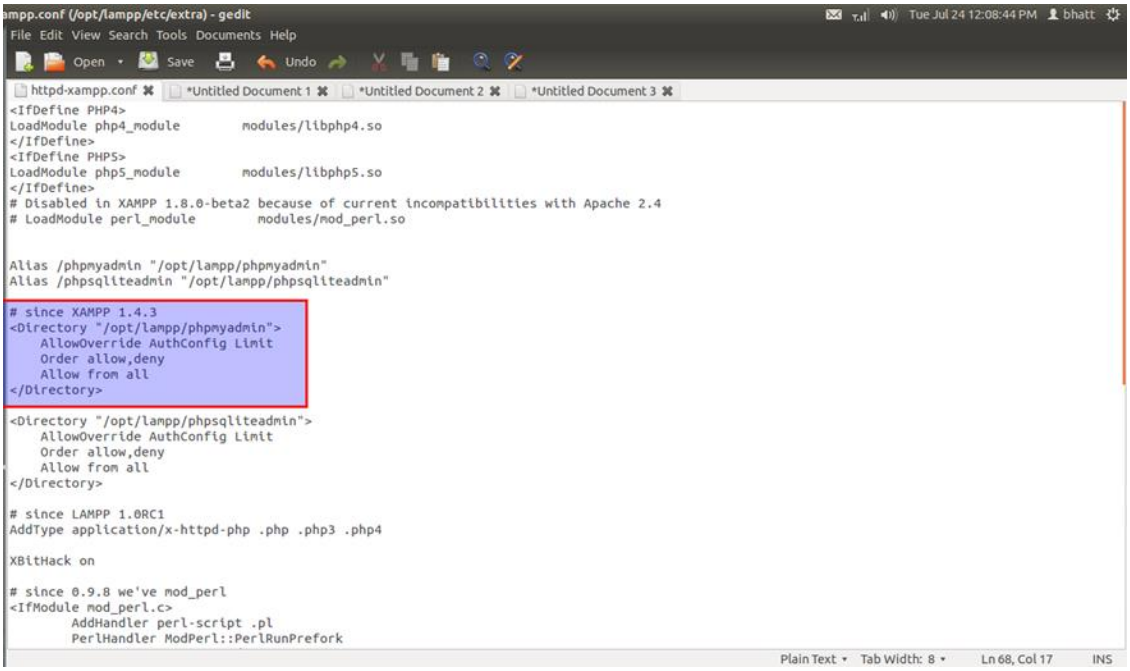

Figura 6
Permisos antes

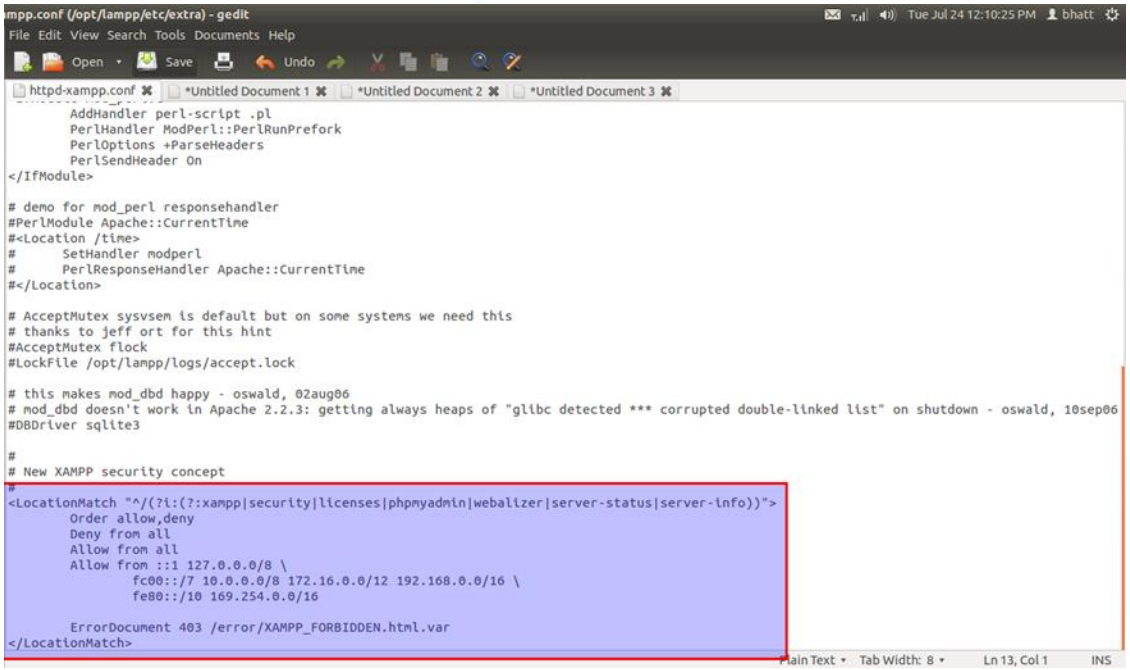

Figura 7
Permisos antes

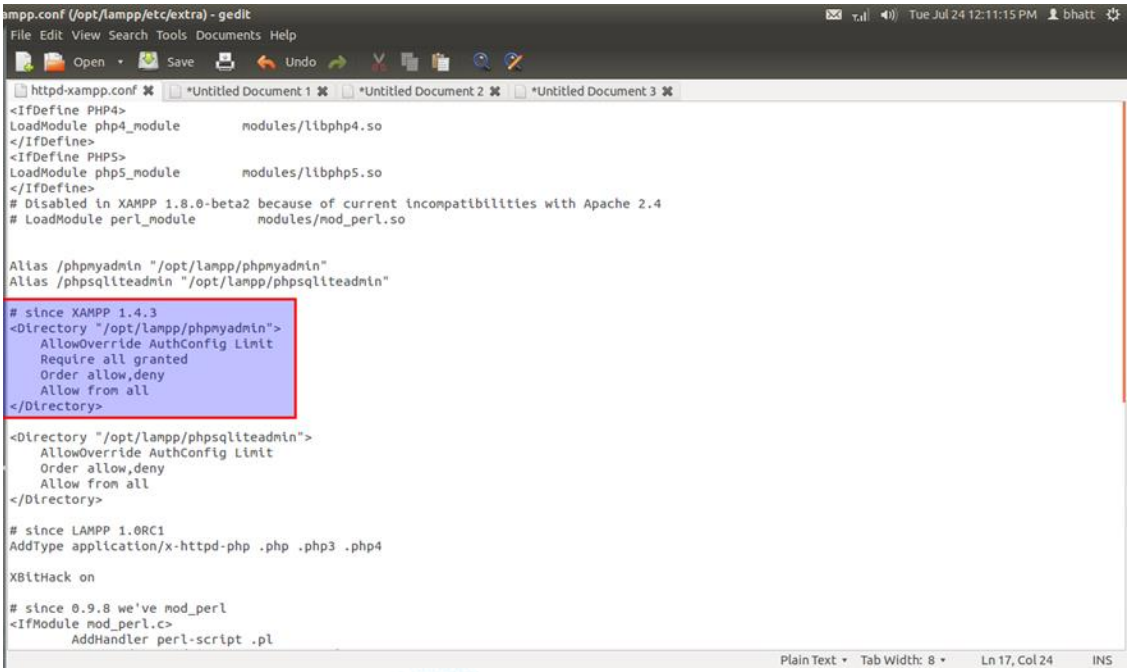

Figura 8
Permisos después

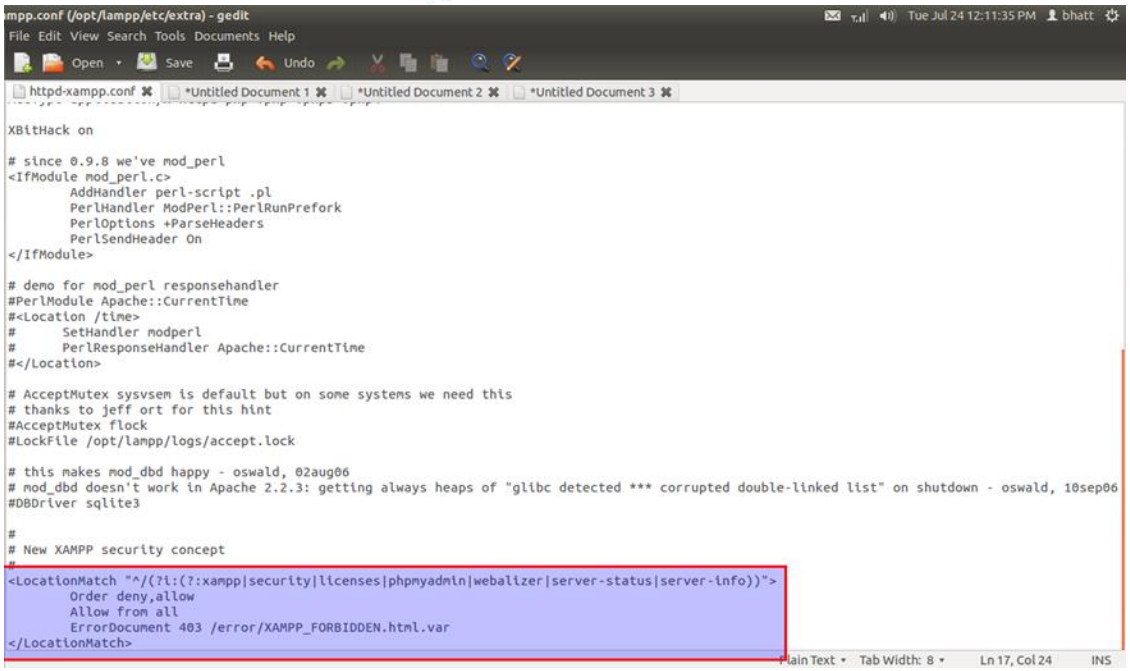

Figura 9
Permisos después

Finalmente, respecto a los permisos, se deben de dar permisos al grupo de ususarios www. Los comandos que en este caso nos ayudarán son:

NOMBRE
groupadd - crear un nuevo grupo

SINOPSIS
groupadd [opciones] grupo

DESCRIPCIÓN
El comando groupadd crea una nueva cuenta de grupo utilizando los valores especificados en la línea de comandos, además de los valores por defecto del sistema. El nuevo grupo se incluirán en los archivos del sistema cuando sea necesario.

OPCIONES
Las opciones que se aplican al comando groupadd son:

-f, - force
Esta opción hace que el comando para salir simplemente con estado de éxito si el grupo especificado ya existe. Cuando se utiliza con-g, y el GID especificado ya existe, otro GID (único) es elegido (es decir,-g se apaga).

-g, - gid GID
El valor numérico de identificación del grupo. Este valor debe ser único, a menos que la opción-o se usa. El valor debe ser no negativo.
El valor por defecto es usar el menor valor de ID mayor que 999 y mayor que todos los demás grupos. Los valores comprendidos entre 0 y 999 son típicamente reservado para las cuentas del sistema.

-h, - help
Muestra el mensaje de ayuda y sale.

-K, - KEY clave = valor
Overrides / etc / defaults (login.defs GID_MIN, GID_MAX y otros). Multiple-K opciones pueden ser especificadas.

Ejemplo: K-GID_MIN = 100-K GID_MAX = 499

Nota: GID_MIN-K = 10, GID_MAX = 499 no funciona todavía.

-o, - no único

Esta opción permite añadir un grupo con un GID no único.

-p, - password CONTRASEÑA
La contraseña de cifrado, tal como lo devuelve crypt (3). El valor predeterminado es deshabilitar la contraseña.

NOMBRE
chmod - cambio bits del modo archivo

SINOPSIS
chmod [OPCIÓN] ... MODE [, MODE] ... Archivo ...
chmod [OPCIÓN] ... OCTAL-modo de archivo ...
chmod [OPCIÓN] ... - Reference = FICHERO FICH_R ...

DESCRIPCIÓN
chmod cambia los bits de modo de archivo de cada fichero dado según modo, que puede ser una representación simbólica de los cambios a realizar, o un número octal que representa el patrón de bits de los bits de modo nuevo.

El formato de un modo simbólico es ugoa [...] [[+ - =] [perms ...] ...], donde las permanentes es o bien cero o más cartas del rwxXst conjunto, o una sola letra de la ugo set. Múltiples modos simbólicos se puede dar, separados por comas.

Una combinación de las letras controles ugoa que será el acceso de los usuarios a los archivos cambiados: el usuario que posee (u), otros usuarios el archivo de grupo (g), otros usuarios no en el grupo del archivo (o), o todos los usuarios (a). Si ninguno de estos se dan, el efecto es como si un se les dio, pero los bits que están activos en la umask no se ven afectados.

El operador + hace que los bits de archivos seleccionados de modo que se añadirán a los bits de modo de archivos existentes de cada archivo, - hace que sean eliminados, y = hace que se añade y hace que los bits no se han mencionado para ser retirado salvo que el usuario set sin mencionar un directorio y bits de ID de grupo no se ven afectados.

Las letras rwxXst bits de selección de modalidad de archivo para los usuarios afectados: lectura (r), escritura (w), ejecutar (o buscar directorios) (x), exe- lindo / búsqueda sólo si el archivo es un directorio o ya tiene permiso de ejecución para algún usuario (X), conjunto de usuario o ID de grupo en ejecución (S), bandera supresión restringido o poco pegajosa (t). En lugar de una o más de estas cartas, se puede especificar exactamente una de las letras ugo: los permisos otorgados al usuario propietario del archivo (u), los permisos concedidos a otros usuarios que

son miembros de la de archivos grupo (g), y los permisos concedidos a los usuarios que se encuentran en ninguna de las dos categorías anteriores (o).

A modo numérico es de uno a cuatro dígitos octales (0-7), derivado de la suma de los bits de valores 4, 2 y 1. Se omiten los dígitos supone que ceros a la izquierda. El primer dígito selecciona los atributos SUID (4) y ID grupo (2) y la supresión restringido o pegajoso (1) atributos. El segundo selecciona los permisos para el usuario que posee el archivo: read (4), escritura (2) y ejecución (1), y el tercero selecciona los permisos para otros usuarios en el grupo del archivo, con los mismos valores, y la cuarta para otros usuarios no está en el archivo de grupo, con los mismos valores.

chmod nunca cambia los permisos de enlaces simbólicos; la llamada al sistema chmod no puede cambiar sus permisos. Esto no es un problema, ya que los permisos de enlaces simbólicos nunca se usan. Sin embargo, para cada enlace simbólico puesto en la línea de órdenes, chmod cambia los permisos de la punta-a archivo. Por el contrario, chmod hace caso omiso de los enlaces simbólicos encuentre durante el recorrido recursivo de directorios.

Es muy importante entender este último comando pues es el que nos permitirá tener mas control sobre la seguridad y las asociación de permisos a grupos de usuarios; los cuales podrían ser asignados a módulos en especifico del sistema, aumentando así la seguridad en archivos y en ejecución/lectura/escritura que generen las peticiones al servidor XAMPP.

A continuación se muestra la Figura 10, que indica cómo cambiar y crear el grupo, para asociarlo satisfactoriamente a una carpeta, o a ciertos usuarios de ciertos permisos. En si, los pasos a seguir serian:

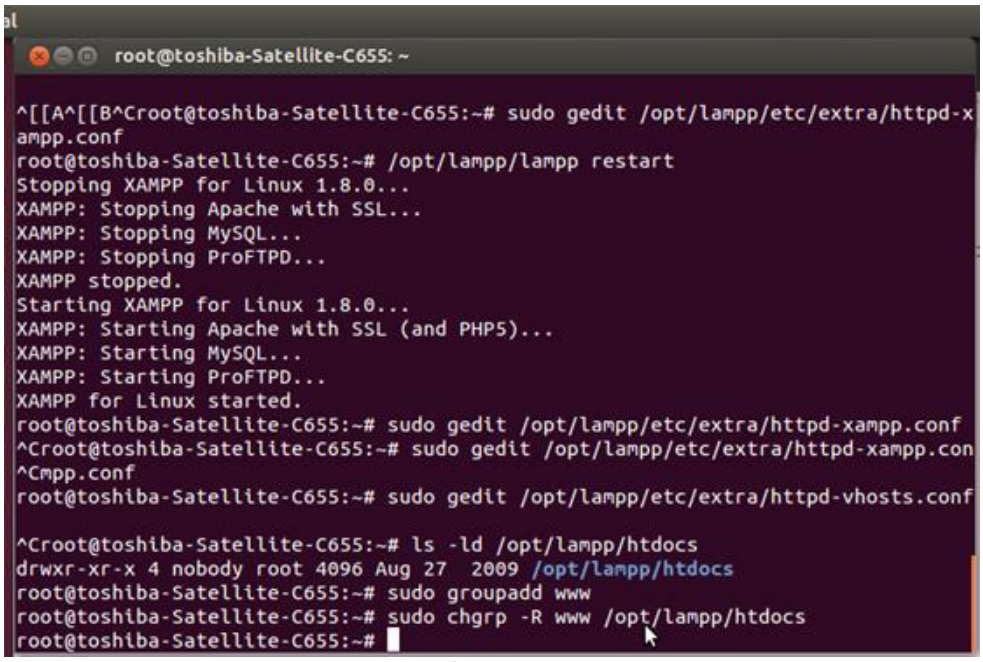

Figura 10
Asignación de permisos de grupo

Hasta este punto ya se agregó el grupo y se le asigno el permiso necesario a htdocs, que es donde colocaremos la aplicación web, para que se puedan ejecutar los scripts que se requieran.

Es importante notar que la disposición de las carpetas donde se colocara la aplicación debe llevar un orden que obedezca a la funcionalidad de cada modulo, pues las reglas de seguridad podrían aplicarse inclusive a nivel de servidor. Teniendo en cuanta que se guardan archivos como fotografías, textos o documentos PDF, se debería analizar a quién se conceden dichos permisos, pues es importante que se lleve un registro de cada acción.

Estos permisos concedidos se refieren a grupos, por que así se pueden asociar dichos elementos en perfiles que pueden parametrizarse mediante el servidor, o mediante la aplicación; interactuando así con la base de datos, se podría tener un bosquejo de log del sistema muy completo, gracias a esto, a nivel de carpeta.

Por otra parte, es relevante notar que las siguientes instrucciones finalizan este esquema de seguridad y permiten dejar el servidor a punto, listo para ejecutar aplicaciones como phpMyadmin.
Los comandos anteriores permiten modificar los permisos de ejecución de los scripts alojados en el servidor.

Fue necesario modificar el archivo htdocs, pues por default no se puede escribir en el por la naturaleza de la carpeta donde se encuentra. La carpeta /opt es considerada como del sistema, por lo tanto se puede hacer uso de un editor de estructura de archivos, *Nautilus*.

Esa relevante mencionar la descripción técnica de este editor para obtener su mayor desempeño en caso de modificar parámetros muy específicos de las carpetas, ya que la principal ventaja de este explorador, es que toma los permisos de usuario Administrador, por lo que deja copiar y pegar dentro de esta carpeta de sistema /opt sin ningún problema.

NOMBRE
nautilus - el administrador de archivos de GNOME

SINOPSIS
nautilus [opciones] URI ...

DESCRIPCIÓN
Esta página del manual documenta brevemente el comando nautilus. Este manual fue escrito para el sistema Debian GNU / Linux porque
el programa original no tiene una página de manual.

Nautilus es el gestor de archivos para el escritorio GNOME.

OPCIONES
Nautilus sigue el orden usual GNU sintaxis de la línea, con opciones largas comenzando con dos guiones ('-'). Un resumen de las opciones se incluye a continuación.

-c

- comprobar
Realice una configuración rápida de la auto-comprobación pruebas.

-g

- geometry = GEOMETRÍA
Crear la ventana inicial con la geometría proporcionada.

-n

- no-default-ventana

Sólo crear ventanas para especificar explícitamente los URI.

- no-desktop
No administrar el escritorio - ignore la preferencia establecida en el diálogo de preferencias.

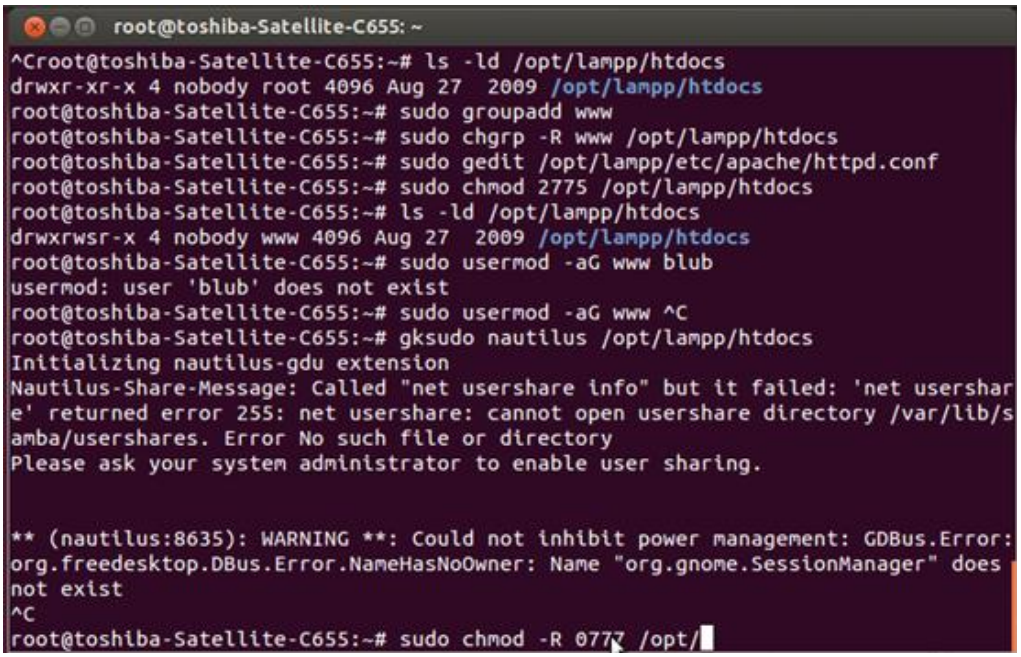

Figura 11
Editor Nautilus

Una vez que este script se completa, se puede acceder libremente a htdocs colocando así, la aplicación SASD en la carpeta correspondiente.

Hasta este punto, los scripts están completos, sin embargo la conexión a la base de datos no se ha realizado, se procede entonces mediante PHPMyAdmin a gestionar la creación de las bases de datos necesarias para la implementación de SASD en el servidor XAMPP en cuestión.

Sera necesario tener listo el archivo de base de datos que fue importado por el respaldo original, para ejecutar una restauración de la base de manera rápida y con un margen de error mínimo, gracias a que phpmyadmin se encargara de gestionar el acceso a la visualización grafica de estos esquemas.

Una vez que se esta en el navegador de internet, dentro del servidor, o en el caso de un acceso externo, remotamente. Se precederá a crear los esquemas de las bases pertinentes mediante PHPMyAdmin.

1.5 Base de datos

A continuación se describe el proceso de instalación de la base de datos del Sistema de Atención de Denuncias e Investigación de Oficio.

Por default se dejaran las opciones de creación, pues la configuración que se podría tomar, ya vendrá en los archivos exportados.

Aunque es pertinente conocer dichas opciones para sacar un mayor provecho a al configuración deseada:

Una vez que se sabe la forma de ingresar comandos, es el momento de acceder a una base de datos.

Suponga que en su hogar posee varias mascotas y desea registrar distintos tipos de información sobre ellas. Puede hacerlo si crea tablas para almacenar sus datos e introduce en ellas la información deseada. Entonces, podrá responder una variedad de preguntas acerca de sus mascotas recuperando datos desde las tablas. Esta sección le muestra como:

La base de datos menagerie (palabra inglesa que en español significa “colección de animales”) se ha hecho deliberadamente simple, pero no es difícil imaginar situaciones del mundo real donde podría usarse un tipo similar de base de datos. Por ejemplo, para un granjero que desee hacer el seguimiento de su hacienda, o para los registros de los pacientes de un veterinario. En el sitio web de MySQL pueden descargarse archivos de texto con datos de ejemplo y algunas de las sentencias empleadas en SASD.

Mediante la sentencia SHOW se encuentran las bases de datos que existen actualmente en el servidor:

```
SHOW DATABASES;
| Database |
+----------+
| mysql    |
+----------+
```

Probablemente la lista obtenida sea distinta en su ordenador, pero es casi seguro que tendrá las bases de datos es necesaria porque es la que describe los privilegios de acceso de los usuarios. La base de datos se provee para que los usuarios hagan pruebas. que si no tiene el privilegio

SHOW DATABASES, no podrá ver todas las bases de datos que hay en el servidor.

Si la base de datos existe, intente acceder a ella:

USE test
Database changed

Advierta que, al igual que QUIT, USE no necesita que ponga un punto y coma al final (aunque puede hacerlo si lo desea). La sentencia USE tiene otra particularidad: debe escribirse en una sola línea.

Puede colocar los ejemplos siguientes en la base de datos, si tiene acceso a ella, pero si trabaja en un ambiente compartido, lo que deposite allí puede ser fácilmente borrado por alguien más que tenga el acceso. Por este motivo, debería pedirle a su administrador permiso para usar una base de datos propia.

De esta manera, se podrían capturar las siguientes bases:

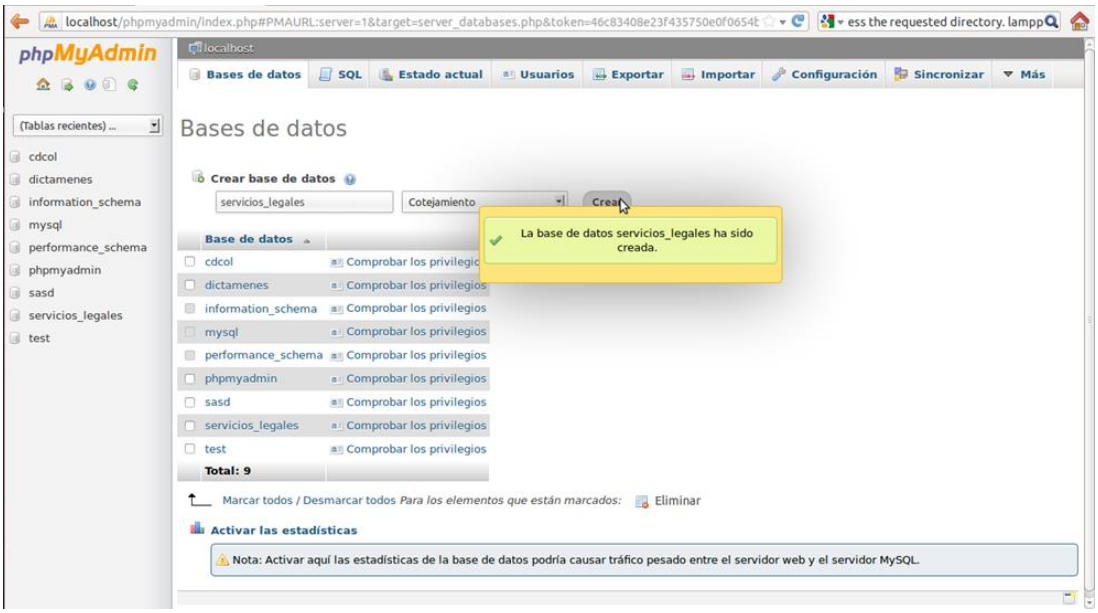

Figura 12
Bases en PHPMyAdmin

Una vez creadas las bases de datos necesarias, se necesita colocar los archivos de la importación del respaldo en las carpetas correspondientes, puesto que todas ellas representan las tablas que cada base contiene, así que se deben pasar íntegramente sin remplazar el archivo de configuración, puesto que la creación de las bases en phpmyadmin le asigno atributos muy específicos acordes a la configuración MySQL donde reside la base de datos.

En la siguiente estructura podemos observar las carpetas ya creadas gracias phpmyadmin, sólo bastaría copiar el contenido de cada carpeta del respaldo en la correspondiente.

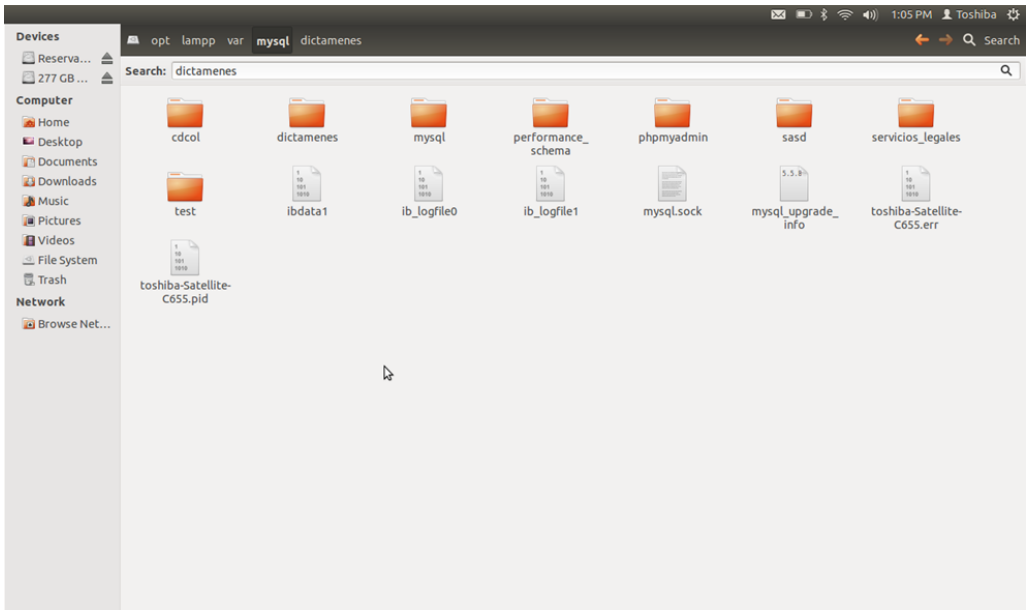

Figura 13
Archivos de bases de datos

1.6 Copia de Scripts

La carpeta de SASD se debe colocar en la carpeta htdocs que se encuentra en /opt/lampp/htdocs/

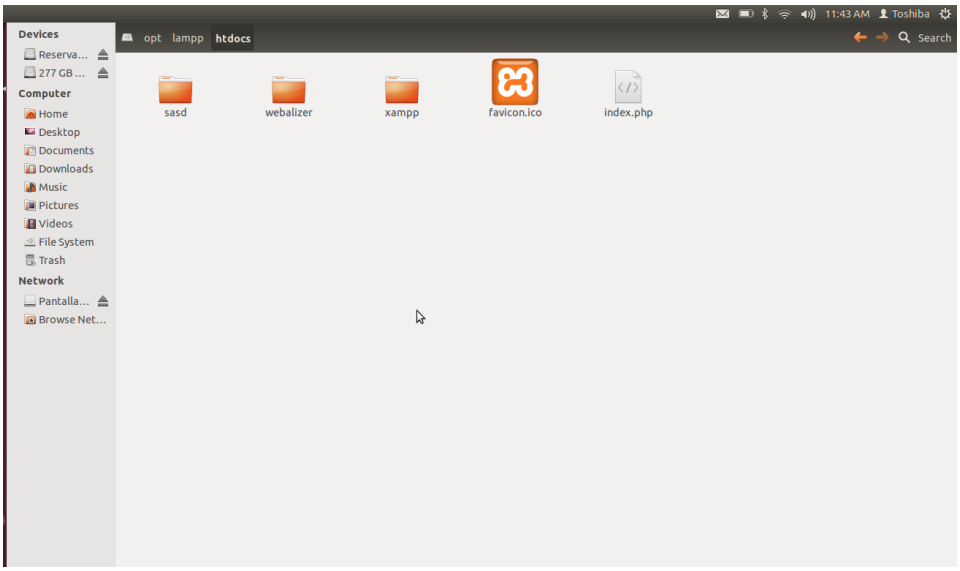

Figura 13
Carpeta sasd en htdocs

1.7 Visualización del sitio SASD

Finalmente, para acceder a SASD basta con ir localmente al navegador a la dirección: http://localhost/sasd/

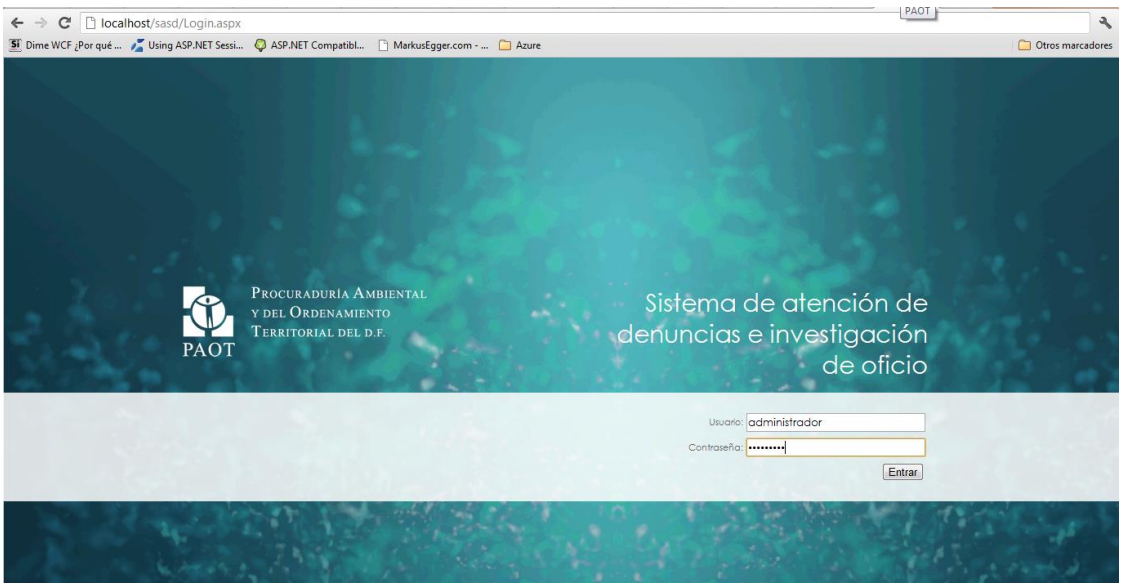

Figura 14
Sitio SASD

Figura 15
Sitio SASD