UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

Colegio de Ciencia y Tecnología

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

"Implementación de las TIC´s en el laboratorio de Ciencias y Tecnologías Sustentables"

PRESENTA:

Giovani Albarrán Núñez

TRABAJO RECEPCIONAL

PARA OBTENER EL TÍTULO DE LICENCIADO EN

INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Director de Tesis:

Dr. José Joaquín Lizardi del Angel

Codirector:

Dr. Rogelio Mendoza Pérez

Ciudad de México, Enero, 2017

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

AGRADECIMIENTOS

Al Laborario de Desarrollo e Investigación de Ciencia y Tecnología Sustentable (LACyTES) del Proyecto: Fondo mixto CONACYT-GDF 2012-2, 189282 por abrirme las puertas a su equipo de trabajo y a todos los que en ese departamento me ofrecieron su apoyo para poder crecer en mi formación académica y hacer posible este logro.

A mi director de tesis, Dr. José Joaquín Lizardi del Angel por haberme otorgado, la confianza, aceptación, paciencia y tiempo en este proceso nuevo de aprendizaje y formación profesional, durante el periodo en el laboratorio LACyTES de la Universidad Autónoma de la Ciudad de México (UACM). Agradezco infinitamente todo su apoyo.

Al Dr. Rogelio Mendoza Pérez por la oportunidad de unirme al proyecto, su paciencia, conocimiento y por todas las enseñanzas académicamente, gracias por todo.

A la Dr. Lester Augusto Alfonso Díaz por sus valiosas aportaciones y sugerencias. Mil gracias por su buena predisposición siempre y compartir su conocimiento y aprendizaje.

A mis compañeros de laboratorio con quienes compartimos día a día durante este trayecto anécdotas, alegrías gracias por hacer ameno este proyecto Kevin Arnoldo Jiménez Gómez, Brenda Hernández Rodríguez, Francisco Cortes Carreón, Marco Antonio Martínez Loredo. Así como a mi amigo Luis Eduardo Medina, por ser una gran persona por su amistad, consejos y conocimiento.

A la Universidad Autónoma de la Ciudad de México quien me dio la oportunidad de realizar uno de mis logros académicos y a todas aquellas personas que comparten conmigo este triunfo.

DEDICATORIAS

A Dios

Por darme salud, fuerza, inteligencia, veracidad, astucia, energía, capacidad, sabiduría para conducir mi camino y por estar conmigo en todo momento gracias.

A mis padres

A mis padres les agradezco el que me hayan brindado la más valiosa de las educaciones disponibles; me refiero a la educación familiar y a los grandes valores morales que me enseñaron con el ejemplo, siempre con una tenacidad y esfuerzos inalcanzables, estos valores se quedaran conmigo toda la vida.

A mi hermano Oscar

Le agradezco ser el modelo a seguir de hermano mayor y por sus esfuerzos al ampliar mi horizonte y mostrarme la variedad y belleza de otros caminos.

Cuando hablo de buenos ingenieros no puedo evitar mencionar su nombre. Por eso quiero agradecer a mi hermano, por ser el ejemplo de éxito profesional que me hizo entender que este éxito depende de uno mismo.

A mi hermano Cristian

Por su forma, por demás valiente y asertiva de tomar decisiones, por llevar a la práctica sus ideas, su fortaleza, disciplina y entusiasmo que han servido como ejemplo en mi vida.

Además ha hecho que ante mis ojos él sea el ejemplo perfecto de vivir de la actividad que te apasiona y solo de trabajar por trabajar. Por todo lo anterior y por ser siempre un vocero de la salud y del bienestar físico, muchas gracias.

A mi hermano Abel

Que anteponiendo su coraje y orgullo siempre me ha acompañado desde la infancia y que ante las situaciones difíciles de la vida siempre ha sabido triunfar y sobresalir gracias a una tenacidad que

permite demostrar con hechos y no con palabras que el éxito de sus proyectos están al alcance de cualquiera cuando se tiene una decisión.

A mi hermano Calos

Por el compañerismo que siempre hemos tenido he el cual ha sido fuente de muchas aventuras lo cual fue maravilloso al crecer con alguien como tú.

“Nunca consideres el estudio como una obligación, si no como una oportunidad para penetrar en el bello y maravilloso mundo del saber” (Albert Einstein).

Contenido

Índice de ilustraciones

CAPITULO 1. INTRODUCCIÓN

Hace algunos años todos los datos e información importante de las organizaciones se almacenaba en papel, generando grandes cantidades de volumen ocupado, ocasionando torpeza como lentitud en el manejo de la información. Hoy en día gracias a los sistemas informáticos es posible la digitalización de la información, logrando mejorar el procesamiento de datos, facilitando su análisis y rapidez de consulta, sin embargo esto ocasiono que personas mal intencionadas intentaran tener acceso a los datos, ya que si es más fácil el transportar la información, también es probable que sea robada o modificada, poniendo en riesgo la integridad y confidencialidad de la información a través de un acceso no autorizado a la red, generando problemas y poniendo en riesgo la integridad de la información.

Debido al creciente y constate uso de internet, más organizaciones y compañías permiten a sus colaboradores y socios acceder a sus sistemas de información. De ahí la importancia de saber que recursos necesitan mayor protección y mantener los derechos y privilegios de los distintos usuarios al nivel de información que le corresponde a cada grupo.

Pues “la información es un activo vital para el éxito y la continuidad de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto un objetivo de primer nivel para la organización y para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización” [1].

Un estudio realizado en 7000 sitios web hechos por WhiteHat Security (Empresa líder en pruebas de seguridad en aplicaciones) el año 2014 arrojó que hay promedio de 230 vulnerabilidades de seguridad informática en cada sitio web aunque hay muchas formas de intentar extraer datos, la mayoría pueden ser evitadas con las medidas de seguridad adecuadas.

La Seguridad informática es una disciplina que comprende e incluye un conjunto de normas y herramientas con el objetivo de garantizar la disponibilidad, integridad y confidencialidad que son los principios para garantizar condiciones seguras y confiables en la protección de la infraestructura

computacional y todo lo relacionado con esta, especialmente la información contenida, así como minimizar los daños de haber en el sistema. Se entiende por confidencialidad a la privacidad de los elementos de información almacenados y procesados en un sistema informático, pues deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. En tanto la integridad garantiza que los datos y archivos sean los que tengan que ser y establece medidas para evitar que sean eliminados o manipulados. Mientras que la disponibilidad se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Para proteger los sistemas se implementan una serie de análisis y aplicaciones con el fin de evitar amenazas potenciales y pérdidas de información, donde a partir de los resultados se tomaran medidas, según sea los niveles de seguridad se implementaran un conjunto de técnicas encaminadas a optimizar los recursos y herramientas para buscar la estabilidad del sistema. Este procedimiento se realizara con base a los niveles de seguridad empezando por las redes informáticas.

1.1 Seguridad en una red informática

Una red es una estructura con el objetivo de compartir recursos como programas, datos y los propios equipos, los elementos que la componen son sobre todo computadoras autónomas pero interconectadas entre sí por medios físicos y/o lógicos que permiten el envío y la recepción de ondas. Estas ondas electromagnéticas llevan los datos que son compartidos por lo tanto, hay emisores y receptores que intercambian mensajes, en cuanto a los medios físicos se necesitan que las computadoras dispongan de una tarjeta de red. Este dispositivo de hardware permite el envío y la recepción de paquetes de datos.

Mientras que los medios lógicos consisten en programas informáticos que establecen protocolos, para que las computadoras se comuniquen entre sí. Estos protocolos envían y reciben grupos de datos denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigiendo el movimiento de paquetes a través de la red física y minimizando

las posibilidades de colisiones entre paquetes enviados simultáneamente. La seguridad en redes consiste en un conjunto de medidas de prevención, detención, y recuperación programadas para enfrentar los riesgos que pueden ser de origen físico, como catástrofes naturales o incendios, de origen humano como sabotaje, robo o hurto y de amenazas lógicas como un virus informático o intrusión, es por eso que se plantearon las siguientes preguntas:

- ¿Qué recursos se quieren proteger dentro de una red?
- ¿De qué se debe proteger?
- ¿En qué grado se necesita proteger?
- ¿Qué medidas y herramientas implantar para tener un óptimo nivel de seguridad sin perder de vista la relación costo/beneficio?

Definidas estas preguntas se implementaron las herramientas y protocolos de seguridad adecuados para crear un perímetro de defensa que permita proteger las fuentes de información sin embargo los recursos a proteger no están estandarizados, dependen de la organización y de los productos o servicios a los que la misma se dedique, básicamente los recursos que se han de proteger son:

a) Software que es el conjunto de programas lógicos que hacen funcional al hardware.
b) Datos que es el conjunto de información lógica que maneja el software y el hardware.

Teniendo en cuenta que cuando se refiere a seguridad en redes el bien más preciado a proteger es la información que circula por la misma.

Por lo que se puede decir que hay tres tipos de mecanismos de seguridad que se abordad en este proyecto los cuales son:

- De prevención: son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo los acosos a la seguridad.

- De detección: se utilizan para detectar violaciones de seguridad o intentos de ello.
- De recuperación: son aquellos que se aplican cuando una violación del sistema se ha detectado y se quiere ponerlo en funcionamiento nuevamente.

En la figura 1.1 muestra un diagrama general sobre la fiabilidad en seguridad en redes donde se observan los aspectos como confidencialidad, Integridad y disponibilidad, así como los elementos a proteger los cuales son hardware, software y datos. También se abordan las amenazas de acuerdo al origen las cuales pueden provenir de personas, ser lógicas o catástrofes naturales otro factor son los mecanismos de prevención, detención y recuperación así como se puede observar.

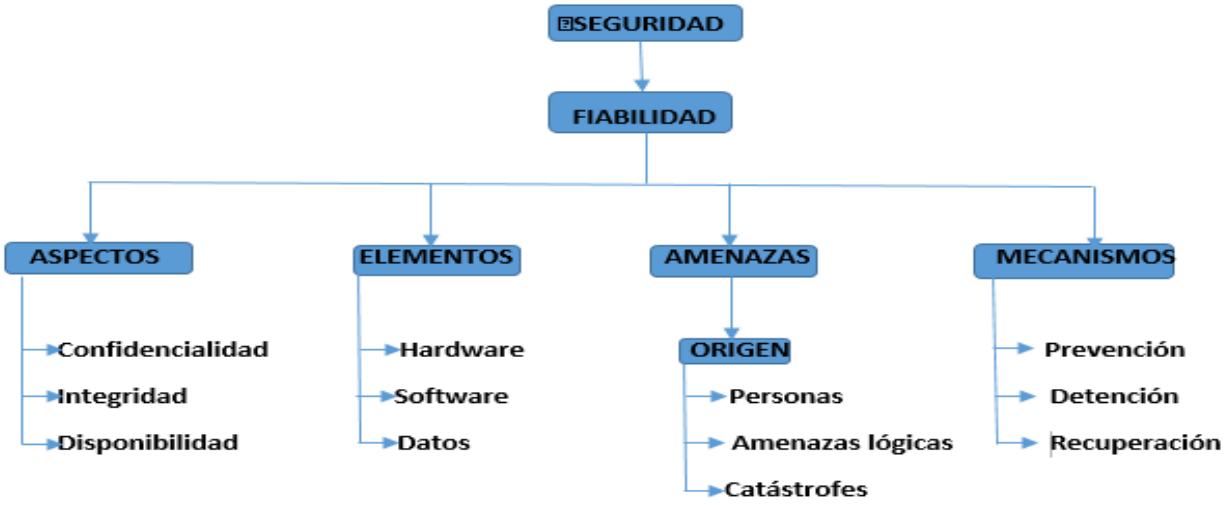


Fig. 1.1 Diagrama de la fiabilidad en la seguridad informática [2]

1.2 Seguridad en un servidor web

Un servidor web es un equipo de cómputo donde se ejecutan procesos para la transferencia de información entre cliente y servidor, manteniéndose a la espera de peticiones de ejecución, el servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados.

Hoy en día, la mayoría de las organizaciones, dispone de su página web. Los servidores web donde se alojan cada una de estas páginas han pasado a ser un blanco fácil para cualquier tipo de atacante con el objetivo de vulnerar los sistemas y obtener información crucial de la organización o simplemente por ocio en busca de fallas en el sistema.

Los “servidores web tienen que estar protegidos frente a cualquier tipo de amenazas y estar preparados para ser el primer punto de entrada” [3], la mayor parte de estos ataques vienen como consecuencia de una mala configuración del servidor o un mal diseño del mismo, así como de fallos de programación.

Por lo tanto existen técnicas y métodos que brindan una seguridad lógica, que consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Como se mencionó anteriormente de los 7000 sitios web analizador por WhiteHat Security en el año 2014 hubo un promedio de 230 vulnerabilidades de seguridad que se encontraban en cada sitio de las cuales las 10 más comunes según WhiteHat se muestran en la Fig. 1.2.

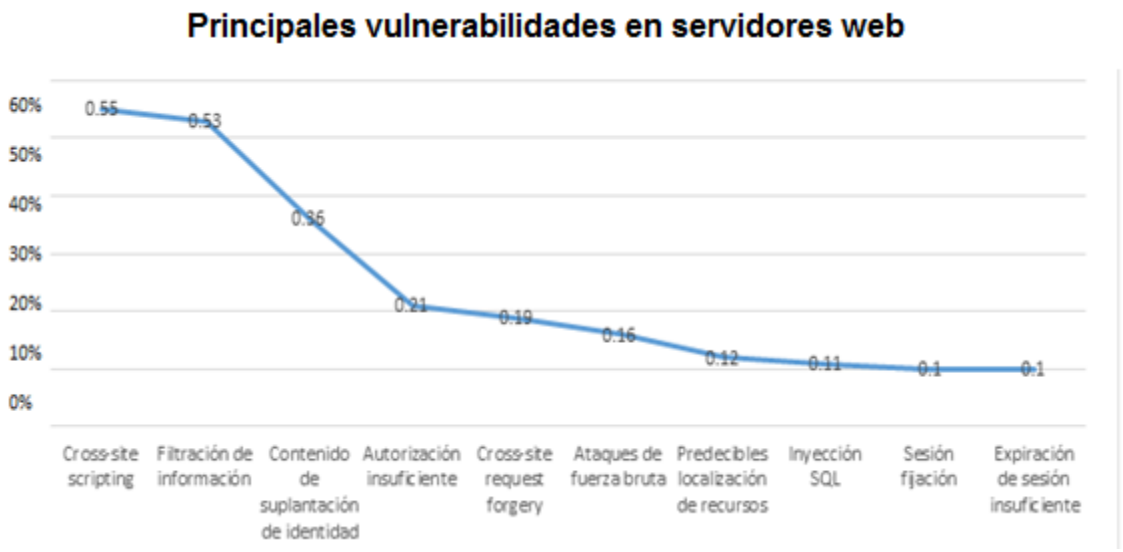


Fig. 1.2 Principales vulnerabilidades en servidores en el año 2015 [4]

- Cross-site scripting (55%)

  "Es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador. Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web, sin estar autenticados en el entorno, nos concede un identificador de sesión, y al autenticarnos el valor de esta sesión no cambia, estaremos ante una vulnerabilidad de fijación de sesión aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, ya sea mensajería instantánea o un correo electrónico. Así mismo, puede provocar una negación de servicio" [5].

- Filtración de información (53%)

  Hoy en día la información contenida en los servidores es uno de los activos más importantes por lo tanto, proteger adecuadamente los datos es fundamental. Dentro de las organizaciones la mayoría de los usuarios no son cocientes de las amenazas o riesgos de compartir cierta información como contraseñas o documentos de investigación.

- Contenido de suplantación de identidad (36%)

  El robo de identidad ocurre cuando una persona se hace pasar por otra utilizando información de ésta con el objetivo de tramitar créditos, tarjetas, préstamos o distintos servicios.
- Autorización insuficiente (21%)

  Sucede cuando en un sitio web permite el aseso al contenido o configuración del sitio sin tener que autenticarse adecuadamente o sin requerir de la forma apropiada la verificación de la identidad del usuario.

- Cross-site request forgery (19%)

  Este ataque forzar al navegador web de su víctima, validando en algún servicio el de enviar una petición a una aplicación web vulnerable. Esta aplicación se encarga de realizar la acción elegida a través de la víctima, debido a que la actividad maliciosa será procesada en nombre del usuario logueado. Al contrario de los ataques conocidos como Cross Site Scripting (su traducción sería ordenes en sitios cruzados – XSS) los cuales explotan la confianza del usuario en un sitio particular; el Cross Site Request Forgery explota la confianza que un sitio web tiene en un usuario particular [6].

- Ataques de fuerza bruta (16%)

  El usuario malicioso utiliza programas informáticos para probar una gran cantidad de contraseñas y descifrar el mensaje o acceder al sistema.
- Predecibles localización de recursos (12%)
- Inyección SQL (11%)

  La inyección directa de comandos SQL es una técnica donde un atacante crea o altera comandos SQL existentes para exponer datos ocultos, sobrescribir los valiosos, o peor aún, ejecutar comandos peligrosos a nivel de sistema en el equipo que hospeda la base de datos.

- Sesión fijación (10%)

  Si una aplicación web, sin estar autenticados en el entorno, nos concede un identificador de sesión, y al autenticarnos el valor de esta sesión no cambia, estaremos ante una vulnerabilidad de fijación de sesión.

- Expiración de sesión insuficiente (10%)

  Mientras que en el 2013 una encuesta de B2B International encargada por Kaspersky Lab (es la empresa privada más grande del mundo y uno de los proveedores de protección TI con mayor crecimiento) ha revelado la siguiente situación.

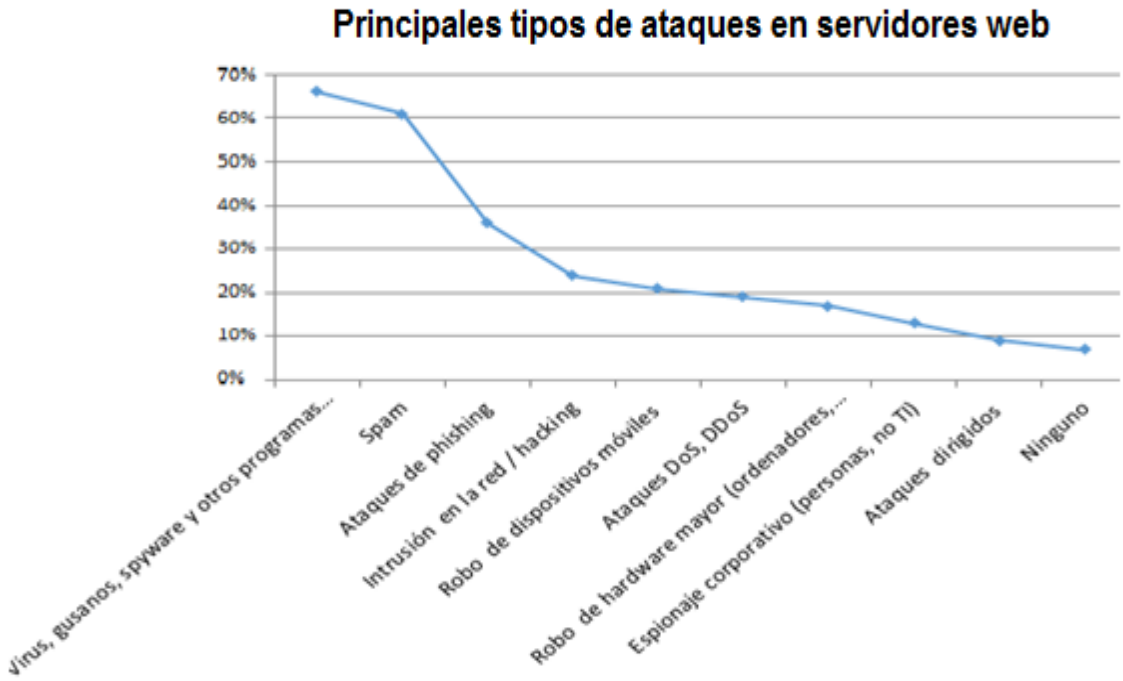


Fig.1.3 Principales tipos ataques en servidores web

Hay muchas formas de intentar extraer datos de un servidor web, pero salvo agujeros graves de seguridad del sistema operativo o del servidor, el atacante necesita conocer un usuario válido y su clave de acceso, y a eso dedicará todos sus esfuerzos. El eslabón más débil de la cadena son los propios usuarios. En efecto casi siempre que lo consiguen es debido al poco cuidado que los usuarios autorizados pues poseen sus contraseñas.

La mayoría de las amenazas contra las cuales lo protegen las soluciones de seguridad pueden ser clasificadas como virus, códigos maliciosos o ataques remotos. Las siguientes definiciones son tomadas del portal de eset.

Virus

Un virus es un programa informático creado para producir algún daño en el equipo y que posee, además, dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Los virus pueden ingresar al equipo desde otras computadoras infectadas, a través de medios extraíbles (CD, DVD, MEMORIA FLAHS etc.) o por medio de una red (local o internet). Existen numerosos tipos de virus, los más comunes son, virus de archivos con extensión .com y .exe, virus script los cuales son desarrollados en VBS, JavaScript, BAT, PHP, etc. Afectan a formatos que contengan HTML y otros que permitan la ejecución de scrips, y finalmente virus Boot que atacan sectores de arranque de los medios extraíbles o del disco maestro.

Gusano

Un gusano es un programa independiente que se replica a través de una red. A diferencia de los virus (los cuales necesitan del archivo infectado para ser copiados y replicarse), el gusano se propaga activamente enviando copias de sí mismo a través de la red local o Internet, así como la comunicación por correo electrónico o aprovechando errores de seguridad del sistema operativo.

Además, pueden propagarse junto a otros códigos maliciosos (instalando programas troyanizados), aunque este comportamiento no se limita estrictamente a los gusanos. Pueden causar un gran daño a menudo se emplean para interferir los canales de comunicación por medio de un ataque DDoS, tiene la capacidad de expandirse mundialmente, vía Internet, en minutos.

Troyano

Un troyano es un código malicioso que, a diferencia de los virus y gusanos, no puede reproducirse por sí mismo e infectar archivos. Usualmente se encuentra en forma de archivo ejecutable (.exe, .com) y no contiene ningún elemento más, a excepción del propio código del troyano. Por esta razón la única solución consiste en eliminarlo.

Adware

El adware es una abreviatura (en inglés) de programas relacionados a la propagación de mensajes

publicitarios. Trabajan mostrando ventanas emergentes durante la navegación en Internet, definiendo varios sitios web como página de inicio o abriendo una ventana especial de interfaz del programa.

Spyware

El spyware es un programa que se vale de Internet para recolectar piezas de información sensible del usuario sin su conocimiento. Algunos de estos programas buscan información tal como la referente a aplicaciones instaladas y al historial de sitios web visitados. Otros programas del tipo spyware son creados con un objetivo mucho más peligroso: la recolección de información financiera o personal para el robo de identidad.

Aplicaciones peligrosas

Se define como aplicación peligrosa a aquel programa legítimo que, habiendo sido instalado por el usuario, podría exponerlo a este a riesgos de seguridad. Ejemplos de estas aplicaciones incluyen keyloggers comerciales o programas para captura de pantalla, herramientas de acceso remoto, programas de pruebas de seguridad y robo de contraseñas.

Hoax

Se denomina hoax a la desinformación deliberada enviada por correo electrónico, y que es difundida con la ayuda de un público desprevenido o desinformado. Son diseñados para incitar al usuario a que realice una acción que no debería ejecutar. Los hoaxes maliciosos a menudo aconsejan a los usuarios eliminar archivos válidos del sistema operativo, argumentando que tal archivo es un virus. En muchos casos remiten a una institución/compañía confiable con el objetivo de llamar la atención del lector. Por ejemplo, " Microsoft advierte que." o "La OMS anunció." Estos mensajes habitualmente advierten acerca de consecuencias desastrosas e incluso catastróficas y cuentan con un elemento común, incitan al usuario a enviar los mensajes a todos sus contactos, lo cual perpetúa el ciclo vital del hoax, ya que el 99.99 % de esta clase de mensajes son engaños.

Los hoaxes no tienen la capacidad de distribuirse por sí mismos. La única manera de protegerse es verificando la autenticidad de cualquier mensaje de correo electrónico antes de realizar cualquier acción que le sea recomendada en el mismo.

Ataques remotos

Son técnicas especiales que permiten a los atacantes comprometer sistemas remotos. Se dividen en varias categorías las cuales son:

DoS, o Denegación de Servicios

Es un intento de deshabilitar un equipo o red para el uso de sus usuarios habituales. Los ataques DoS obstruyen las comunicaciones entre los usuarios afectados, impidiendo que continúen siendo funcionales. Un método frecuente de ataque implica la saturación del equipo vulnerado con solicitudes de comunicaciones externas, de modo que este no pueda responder al tráfico legítimo o lo haga con tal lentitud que se la considere no disponible. Estos ataques usualmente conducen a una sobrecarga del servidor. Los equipos expuestos a ataques suelen requerir el reinicio para así poder funcionar apropiadamente. Los objetivos de los ataques DoS son los servidores web y el propósito es que permanezcan inhabilitados para los usuarios durante un período determinado.

Envenenamiento de DNS

Valiéndose del envenenamiento de DNS (Domain Name Server) los hackers pueden engañar al servidor DNS de cualquier equipo logrando fingir que la información falsa es legítima y auténtica. Esta última es almacenada por un período determinado, permitiendo a los atacantes reescribir las respuestas de DNS de las direcciones IP. Como resultado, los usuarios que intentan acceder a los sitios web cuyos DNS fueron envenenados descargarán en sus equipos virus o gusanos en lugar del contenido originalmente publicado.

Desincronización de TCP

La desincronización de TCP (Protocolo de Control de Transmisión) es una técnica empleada en ataques de "secuestro" de TCP. Se desencadena mediante un proceso en el cual el número secuencial de los paquetes entrantes difiere del número secuencial esperado. Los paquetes que tienen un número secuencial diferente son rechazados (o guardados en un búfer de almacenamiento si se encuentran presentes en la ventana de comunicación actual). En la desincronización, ambos puntos de comunicación desestiman los paquetes recibidos, lo cual habilita a los atacantes remotos infiltrar y proveer paquetes con un número secuencial correcto. De ese modo pueden manipular o modificar la comunicación.

Ataques de "secuestro" de TCP propician la interrupción de las comunicaciones entre servidor-cliente. Muchos ataques pueden ser evitados mediante el uso de autenticación para cada segmento TCP.

Ataques ICMP

ICMP (Protocolo de Mensaje de Control de Internet) es un protocolo de Internet popular y ampliamente utilizado, principalmente por equipos puestos en red, para enviar varios mensajes de error.

Los atacantes remotos intentan explotar la debilidad del protocolo ICMP, el cual fue diseñado para comunicaciones de una sola dirección que no requieren autenticación. Esta condición habilita a los atacantes a desencadenar ataques DoS (Denegación de Servicios), o ataques que brindan a individuos no autorizados acceso a los paquetes entrantes y salientes. Ejemplos recurrentes de un ataque ICMP son los ataques por flujo de ping, por flujo ICMP_ECHO y de "pitufos". Los equipos expuestos a un ataque ICMP experimentarán muy bajo rendimiento en las aplicaciones que utilizan Internet, además de problemas de conexión. Así pues, además de cuidar con esmero las claves de acceso, lo primero que se buscara es cerrar todas las puertas que no sean necesarias del servidor. En un servidor web lo típico necesario suele ser el propio servicio HTTP (Protocolo de Transferencia de Hipertexto) puerto 80, y el de FTP (Protocolo de Transferencia de Archivos) puertos 20 y 21, además de esto se analizará si se cierran o a se dejan abiertos más puertos los cuales se encuentran en el anexo 1.

1.3 Seguridad en un Cortafuegos

El cortafuego es una herramienta de supervisión y prevención la cual analiza el tráfico direccionando y estableciendo criterios de ruteo, así como adecuado la comunicación, uso y acceso a los sistemas dentro de la red. En la prevención se establecen las reglas para usos atípicos de la información, así como liberar sobrecargos y establecer bloqueos al denegar acceso a puertos que no están en uso.

Puede ser software, hardware o una combinación de ambos teniendo como base un conjunto de normas y reglas. Todos los mensajes que entren o salgan de la intranet deben pasar a través del cortafuegos que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. Es recomendable conectar el cortafuegos a una tercera red llamada zona desmilitarizada (DMZ), en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Para el presente trabajo se delimitaron las características del cortafuego de acuerdo a las cualidades del proyecto que al final de este capítulo se especificarán.

1.4 Seguridad en bases de datos

En una base de datos se almacenan la información valiosa y confidencial de una organización pues la mayoría de los datos del mundo están almacenados en sistemas gestores de base de datos y es por eso que se emplean un conjunto de directivas personalizables para alcanzar la una seguridad y conformidad eficientes de acuerdo a las necesidades de este proyecto.

De acuerdo con AppSec's Team SHATTER (Security Heuristics of Application Testing Technology for Enterprise Research), alrededor de la mitad de las vulnerabilidades nombradas a continuación, están directa o indirectamente relacionadas con las prácticas flojas de gestión de parches en el entorno de base de datos. Dentro de este estudio se encontró las 10 vulnerabilidades más comunes las cuales son:

1.- Nombre de usuario/password en blanco, por defecto o débil

Es típico encontrar nombres de usuarios y contraseñas débiles, esta es la primera línea de defensa y es por eso importancia en hacer revisiones periódicas de credenciales.

2.- Inyecciones SQL

Cuando la plataforma de base de datos falla para desinfectar las entradas, los atacantes son capaces de ejecutar las inyecciones SQL de forma similar a como lo hacen en los ataques basados en Web, lo que permite elevar sus privilegios y obtener acceso a una amplia gama de funcionalidades [7].

3.- Preferencia de privilegios de usuario por privilegios de grupo

Garantizar que los privilegios no se les den a los usuarios por asignación directa se recomienda que los usuarios sólo reciban privilegios por parte de grupos o funciones y sean manejados colectivamente. De esta forma será más fácil eliminar derechos a un usuario con simplemente eliminarlo del grupo, sin que queden derechos ocultos u olvidados asignados a dicho usuario.

4.- Características de base de datos innecesariamente habilitadas

La instalación de base de datos viene con paquetes adicionales de todas las formas y tamaños que en su mayoría rara vez son utilizados por una organización. En materia de seguridad de base de datos es de suma importancia el reducir las superficies de ataque, por lo que se necesita buscar los paquetes que no se utilizan y desactivarlos. Esto no sólo reduce los riesgos de ataques a través de estos vectores, sino que también simplifica la gestión de parches.

5.- Configuración de seguridad ineficiente

La base de datos tiene una gran cantidad en opciones de configuración y consideraciones diferentes a disposición del administrador para ajustar el rendimiento y funcionalidades mejoradas. Las organizaciones necesitan conseguir y desactivar aquellas configuraciones inseguras que podrán estar activadas por defecto para mayor comodidad de los DBA (Administrador de Bases de Datos) o desarrolladores de aplicaciones. Las configuraciones de bases de datos en producción y desarrollo deben ser radicalmente diferentes.

6.- Desbordamientos de búfer

Las vulnerabilidades de desbordamiento de búfer, son explotadas por las inundaciones de las fuentes de entrada con valores diferentes o muy superiores a los que la aplicación está preparada.

7.- Escalada de privilegios

Las bases de datos con frecuencia exponen vulnerabilidades comunes que permiten a un atacante escalar privilegios en una cuenta de bajos privilegios hasta tener acceso a los derechos de un administrador. A medida que estas vulnerabilidades son descubiertas, los proveedores las corrigen y el administrador debe mantener las actualizaciones y parches actualizados.

8.- Ataque de denegación de servicio

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

9.- Bases de datos sin actualizar

Esta vulnerabilidad aparece si no se aplican un parche en el momento oportuno por el riesgo de que este dañe la base de datos. Pero el riesgo de ser hackeado es mucho más alto que el riesgo de aplicar un parche que descomponga la base de datos.

10.- Datos sensibles sin cifrar, tanto en reposo como en movimiento

El cifrado es una operación criptográfica reversible que transforma datos significativos sin proteger, conocidos como texto sin formato, en datos ilegibles y cifrados (conocido como texto cifrado), utilizando una clave llamada clave de cifrado.

Teniendo en cuenta la siguiente información y las características del proyecto que continuación se tomaron y evaluaron medidas para poder tener un control con seguridad en la base de dados acuerdo a las necesidades planteadas en los siguientes capítulos para la integridad de la información.

En el Laboratorio de Ciencias y Tecnologías Sustentables (LACyTES) apoyado por el CONACyT y proyectos de convocatoria interna de la Universidad Autónoma de la Ciudad de México (UACM) se lleva a cabo la manufactura de módulos fotovoltaicos de CdS/CdTe en áreas de 100 cm2 por la técnica de sublimación y procesos preindustriales asociados, en donde se requiere un mejor manejo de la información en los datos de los procesos relacionados a los experimentos propios de la actividades de docencia, difusión e investigación que se llevan a cabo en el lugar. Para salvaguardar la información y mejorar la adquisición de datos se realizó una implementación de seguridad, que se detallará a continuación:

Se creó una red de infraestructura para el laboratorio que provee a los usuarios de conectividad adecuada tanto a equipos de uso común como de equipo especializado conectado a red. Esta instalación prevé distintos niveles de conectividad que van desde aquellos que se enlazan a red cableada, a conexiones de usuarios a la red inalámbrica de este laboratorio para usuarios foráneos y dispositivos móviles.

La programación de un desarrollo web en donde los investigadores y estudiantes que están involucrados en dicho proyecto puedan almacenar y dar seguimiento de sus datos a través de una bitácora electrónica de sus experimentos que les permita consultar resultados desde cualquier lugar fue implementado. Así como realizar el despliegue de diferentes graficas respecto a ciertas etapas de la muestra, lo cual dependerá de los privilegios con los que cuente el usuario, ya que la información desplegada depende de los permisos de éste.

Así mismo se realizaron distintos tipos de redes para alojar los distintos servicios que proveerán al laboratorio. Una de ellas es la zona DMZ (zona desmilitarizada), red donde se establecieron los mayores parámetros de seguridad dado que en ella se alojaran los servidores necesarios para este fin, y otros con objetivos académicos y de investigación asociados a este laboratorio.

Bajo estas características, se buscarán las herramientas que permitan cumplir los objetivos de forma segura logrando la disponibilidad, integridad y confidencialidad de la información y de datos generados en LACyTES.

1.5 Organización de la Tesis

En el capítulo II, se hablará de la seguridad en redes y la implementación de un cortafuegos que se adapta y cumple con los estándares de seguridad protegiendo y resguardando la información e integridad de las redes en el laboratorio, permitiendo dar la confianza de que la información esta guardada de una forma trasparente y segura.

En el capítulo III, se tratarán las generalidades en la instalación de un servidor web, para ello se realizó una comparación entre las diferentes distribuciones de Linux escogiendo la que mejor se adaptó con base al costo, seguridad, entorno y actualización, así como aplicación y base de datos tomando en cuenta la implementación de la página con el objetivo de contar con un servidor de datos robusto y confiable.

En el capítulo IV, se detallara el trabajo realizado para realizar la implementación de un servicio web a la medida que permita a los usuarios del laboratorio dar seguimiento a los procesos experimentales propios de la manufactura de la celda solar.

En el capítulo V, se abordarán las conclusiones del trabajo, así como las recomendaciones y las posibles mejoras a fututo de la implementación antes mencionada.

CAPÍTULO 2. IMPLEMENTACION DEL CORTAFUEGOS

Para mejorar la seguridad conservando la integridad de los datos e información sin perder la disponibilidad se implementó un contrafuegos, para esto se llevó a cabo una investigación tomando en cuenta las características del laboratorio de LACyTES y las del cortafuegos que enseguida se describirán, así como la razón de su implementación.

2.1 Sistema operativo (Pfsense)

Pfsense es una distribución personalizada de FreeBSD la cual es un sistema operativo multiusuario, capaz de efectuar multitareas con apropiación y multiproceso en plataformas compatibles con múltiples procesadores. Adaptado para su uso como firewall, enrutador, y servidor de balanceo de carga entre otras, con una interface amigable.

Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de ordenadores, y además cuenta con una interfaz web sencilla para su configuración. El proyecto es sostenido comercialmente por BSD la cual lo hace una distribución libre de acuerdo al portal oficial de Pfsense. Para el 2010, Pfsense ha tenido más de un millón de descargas donde ha sido instalado con éxito en ambientes desde redes domésticas hasta grandes corporaciones.

Siendo una aplicación que se instala como un sistema operativo, tiene varias funcionalidades entre estos servicios de redes LAN y WAN (Red de Área Amplia). Estos servicios de acuerdo al manual de Pfsense 2011son los siguientes:

Firewall:

Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también hace filtrado avanzado de paquetes por protocolo y puerto.

Servidor VPN:

Pfsense se puede configurar como un servidor VPN (Red Privada Virtual) usando protocolos de tunneling tales como IPSec (Internet Protocol security), PPTP (Protocolo de túnel punto a punto), entre otras.

Servidor de Balanceo de Carga:

Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo y de DNS. También para proveer estabilidad y redundancia en el envió de tráfico a través del enlace WAN, evitando los cuellos de botella.

Portal Cautivo:

Este servicio consiste en forzar la autenticación de usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago, etc. Y para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

Tabla de estado:

Pfsense tiene como característica principal que guarda el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado.

Servidor DNS y reenviador de cache DNS:

Se puede configurar como un servidor DNS primario y reenviado consultas de DNS.

Servidor DHCP (Protocolo de Configuración de Host Dinámico):

También funciona como servidor de DHCP, se puede también implementar VLAN (red de área local virtual) desde Pfsense.

Servidor PPPoE (Protocolo Punto a Punto sobre Ethernet):

Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local.

Enrutamiento estático:

Pfsense funciona como un enrutador ya que entrega direccionamiento IP y hace el nateo hacia afuera.

Redundancia:

Pfsense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae, el otro se declara como cortafuegos primario.

Reportes y Monitoreo:

A través de los gráficos, Pfsense muestra el estado de los siguientes componentes:

Utilización de CPU.

Rendimiento Total.

Rendimiento individual por cada interface.

Paquetes enviados y recibidos por cada interface.

Manejo de tráfico y ancho de banda.

2.2 Instalación de Pfsense

Una vez que se han investigado y valorado las características de Pfsense se procedió a la instalación. Lo primero que se realizó fue descargar una versión estable del sitio oficial, al tener a la mano la imagen de Pfsense versión 2.2.6 se comenzó con la instalación siguiendo los siguientes pasos, que a continuación se muestran.

El primer cuadro de dialogo con Pfsense mostrando el menú principal de instalación que se observa en la siguiente imagen.

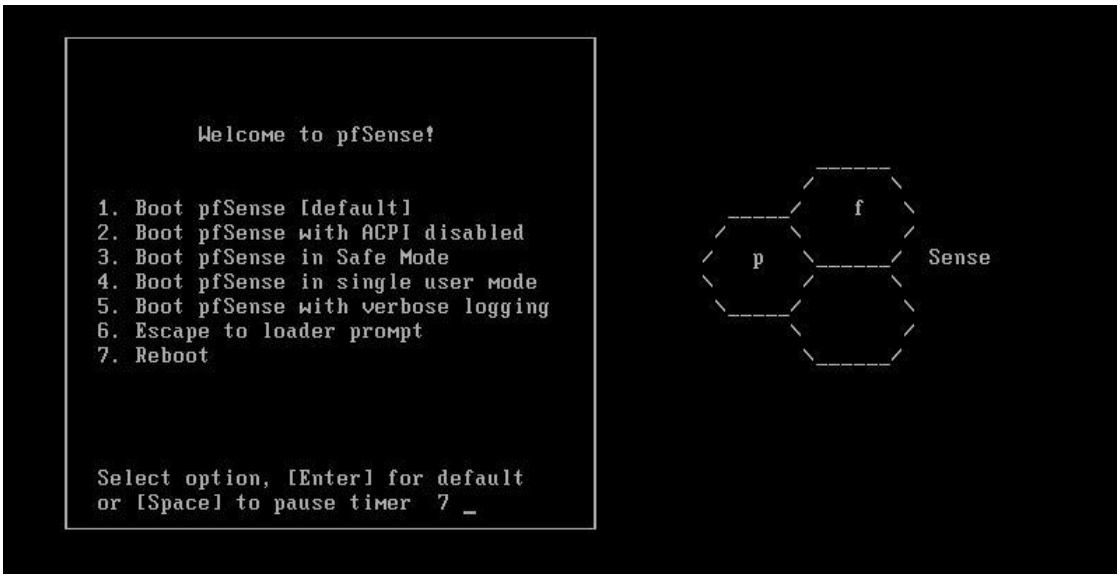


Fig. 2.1 Primer menú para la instalación de Pfsense

La primera pregunta es si se desea crear VLAN, y se eligió n para crearlas más tarde.

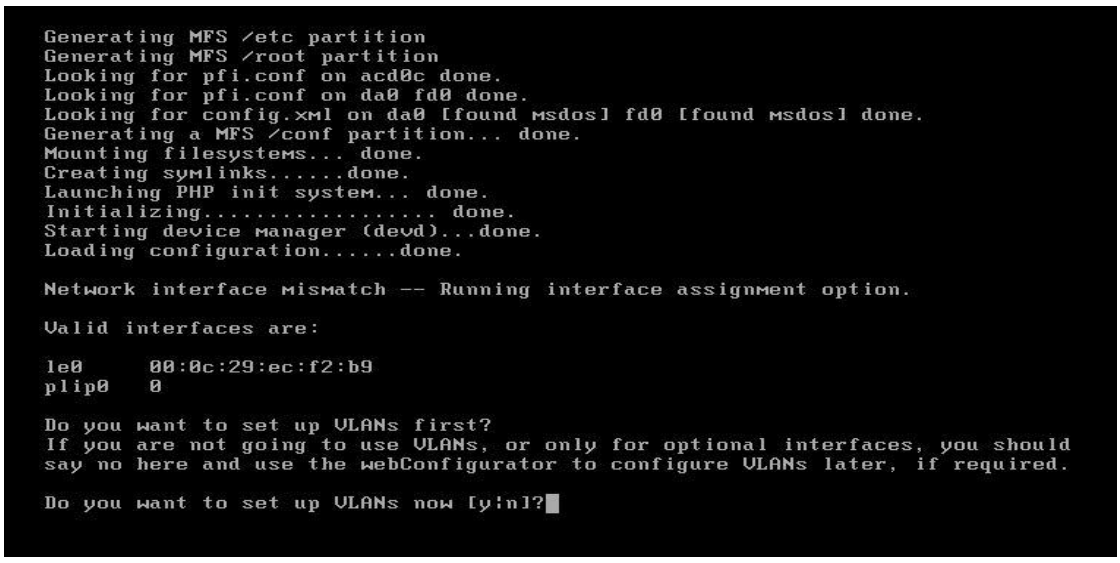


Fig. 2.2 Selección de VLAN y sus valores en Pfsense.

Este es el paso donde el sistema identifica las interfaces LAN y WAN, seleccionando que tarjeta va hacer WAN y cual LAN, Las ips asignadas a cada tarjeta se pueden cambiar, en este caso esta solo es para hacer la instalación más adelante y se modificarán de acuerdo a las necesidades del proyecto.

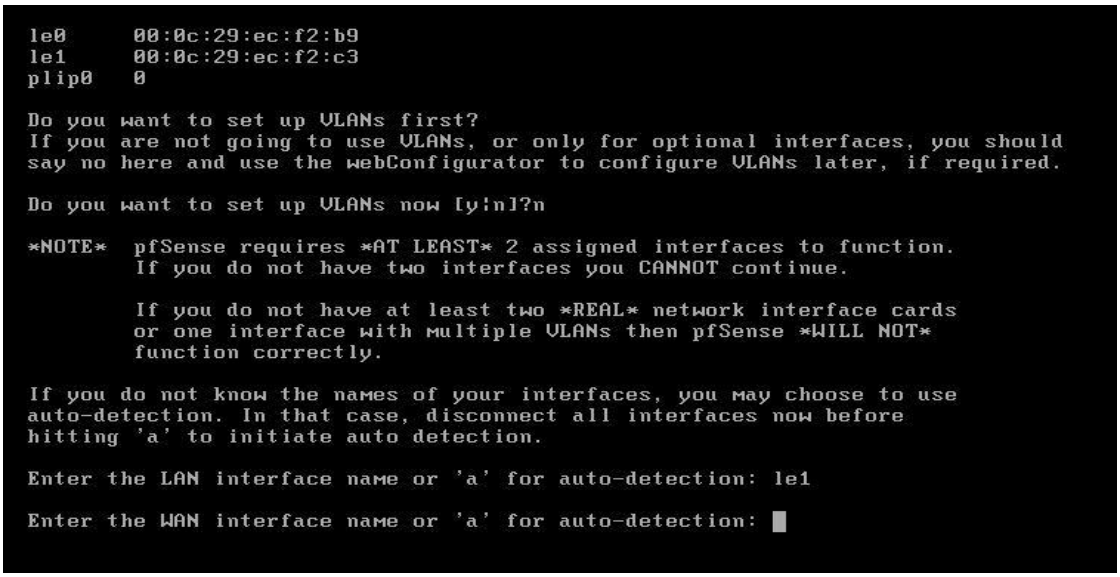


Fig. 2.3 Selección de interfaces LAN y WAN para cada tarjeta de red

En este menú se escoge la opción 99, lo cual iniciaría el asistente de instalación.

Fig. 2.4 Fin de la preinstalación de Pfsense en el equipo asignado y valores mínimos configurados

Después de seleccionar la tarjeta de video, se procedió a la instalación.

Fig. 2.5 Inicio de la instalación de Pfsense

En este paso se comienza a dar la instalación por completo, así mismo en este punto se hace el formateo del disco y el particionado del mismo.

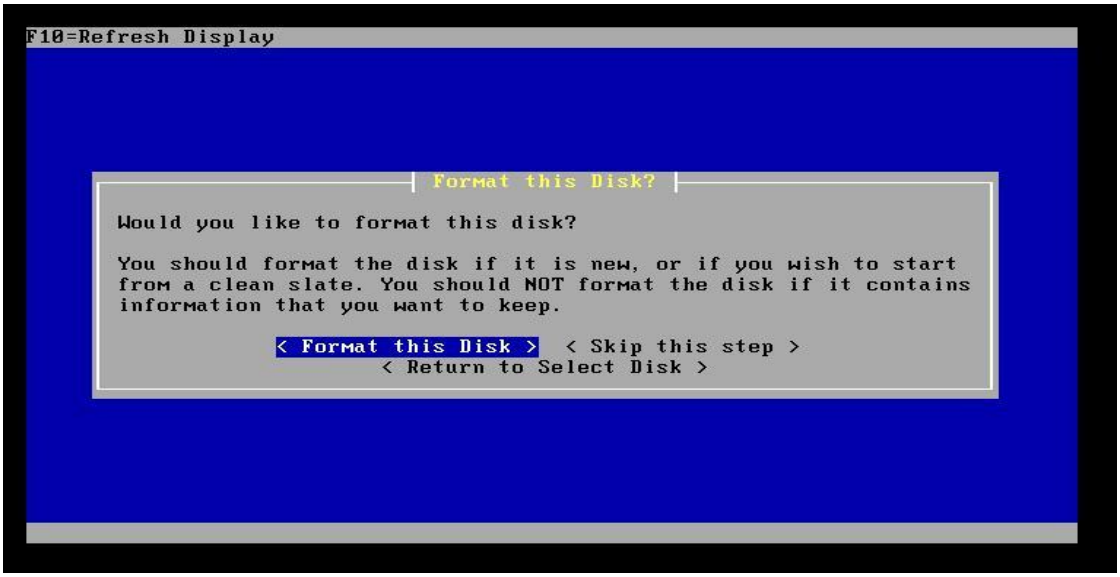


Fig. 2.6 Formateo del disco duro

Una vez copiados todos los archivos al disco duro, prácticamente se instala Pfsense en el equipo.

Fig. 2.7 Fin de la copia de archivos y datos a disco duro de Pfsense

Se reinicia finalizando la instalación, más no configuración.

Fig. 2.8 Configuración básica de Pfsense en modo web

Una vez que se termina la instalación, se procedió a configurar las directivas y protocolos para tener un cortafuego que proporcione disponibilidad, integridad y confidencialidad en la red. Esta configuración se abordara a continuación.

2.3 Directivas y Protocolos de Pfsense

Como se explicó en el capítulo anterior a mayor detalle el cortafuegos es una herramienta de supervisión y prevención la cual analiza el tráfico direccionando y estableciendo criterios de rooteo, así como adecuado la comunicación, uso y acceso a los sistemas dentro de la red. Sin embargo, la eficacia con la que este cumpla esta función depende de las directivas y protocolos adecuados y personalizados al uso y requisitos de la red así como sus servicios, usuarios e información en esta. A continuación se muestran un diagrama de la red así como los protocolos y directivas.

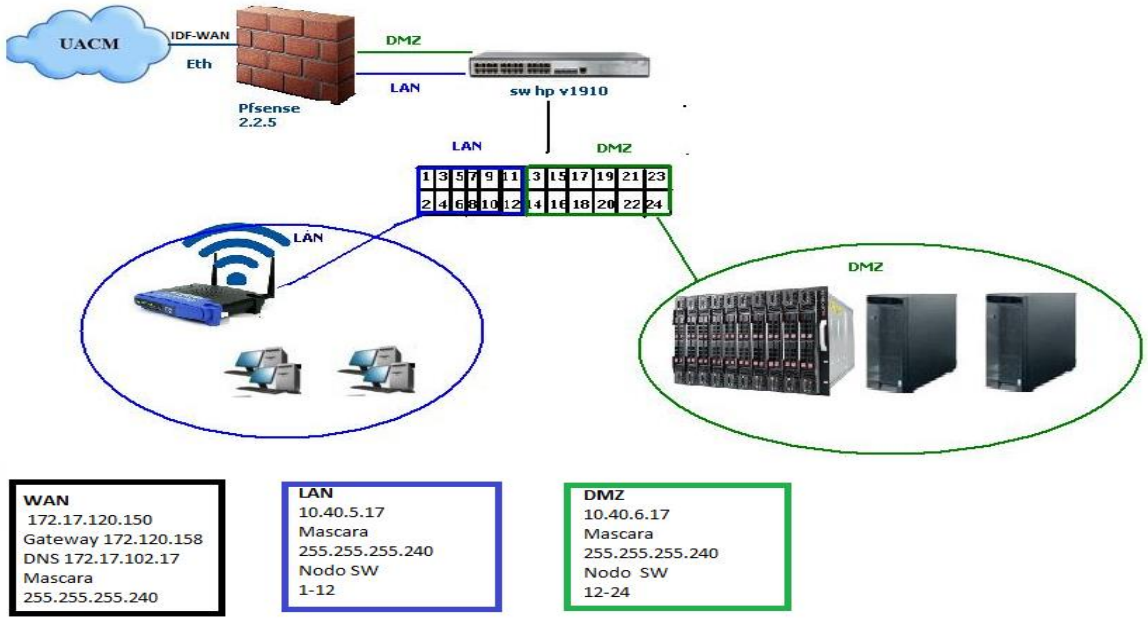


Fig. 2.9 Diagrama de la red del laboratorio LACyTES donde se muestra la asignación de VLANs

En esta red, se implementaron de dos VLANs tanto en Pfsense como en el switch, una para desarrollo e investigación y otra para la DMZ que es una red aislada del resto de la red interna, donde se ubican únicamente los servidores que deben ser accesibles desde Internet, de esta forma si se ataca y compromete uno de estos servidores, el resto de la red estará protegida.

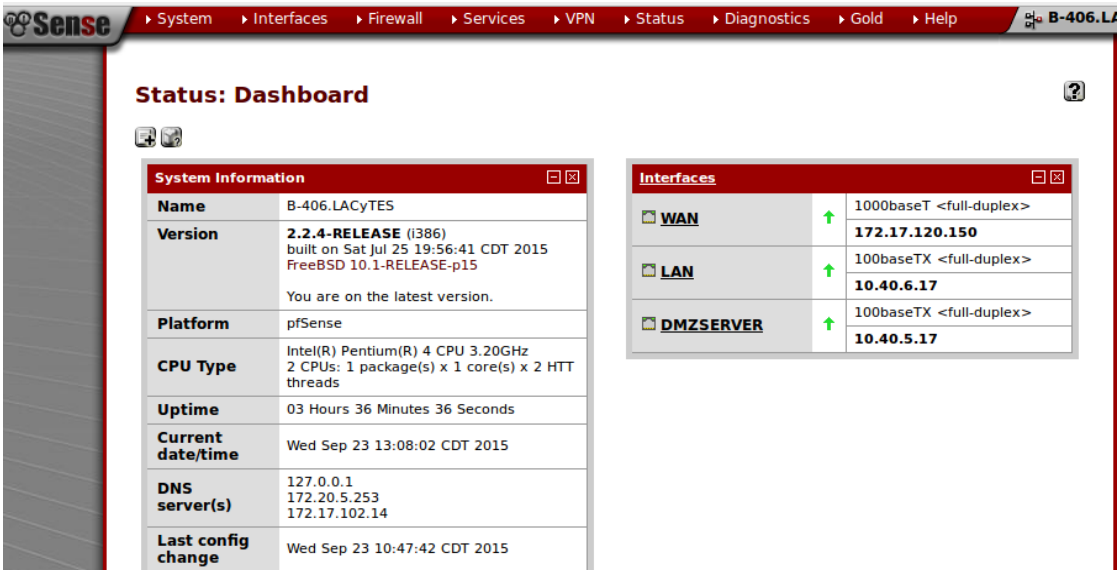


Fig.2.10 Características básicas de Pfsense

Otro factor que se utilizo fue el filtrado MAC (Media Access Control) en cada VLAN para controlar los dispositivos que tengan acceso a la red es decir se creó una lista de dispositivos. Tomando en cuenta las necesidades y características del usuario para que al mismo tiempo no sea una fuente de peligro dentro de la red, esto permite la conexión a los dispositivos añadidos a la lista de direcciones MAC, quedando cualquier otro sin posibilidad de conectarse a nuestra red. Esto es bastante útil ya que solo unos determinados dispositivos puedan conectarse a nuestra red.

DHCP Static Mappings for this interface.

Static ARP	MAC address	IP address	Hostname	Description
	c8:1f:66:2f:5a:12	10.40.6.18	Nodo_A	PC-Felix
	c8:1f:66:2c:98:23	10.40.6.19	Nodo_B	PC-Libre
	c8:1f:66:27:f2:d9	10.40.6.20	Nodo_C	PC-Kevin
	c8:1f:66:2f:59:81	10.40.6.21	Nodo_D	PC-Erendida
	c8:1f:66:2f:59:07	10.40.6.22	Nodo_E	PC-Libre
	00:23:69:ad:c2:8c	10.40.6.24	Wireless	Ap-LACyTES

Fig. 2.11 Filtrado por MAC en la VLAN en Pfsense

DHCP Static Mappings for this interface.

Static ARP	MAC address	IP address	Hostname	Description
	00:26:6c:97:67:18	10.40.5.18	Nodo_1	Laptop-Ocram
	10:78:d2:c3:c5:7e	10.40.5.19	Nodo_2	PC-Brenda
	c8:0a:a9:39:4f:2d	10.40.5.20	Nodo_3	Laptop-Gio
	e0:3f:49:49:87:04	10.40.5.21	Nodo_4	PC-LUFAc
	84:8f:69:f5:95:70	10.40.5.22	Nodo_5	PC-AlienWare
	00:25:90:d6:c5:c0	10.40.5.23	Nodo_6	Serv-SM
	40:6c:8f:b7:b7:07	10.40.5.24	Nodo_7	LACyTES

Fig. 2.12 Filtrado por MAC en la DMZ en Pfsense

En la edición de las reglas se decidió qué conexiones se permiten y cuáles no, así como si un paquete de información puede entrar, por lo tanto en lo que se refiere a las salidas, sólo dejare abiertos aquellos puertos que sean de utilidad todos los demás se decidieron cerrar.

En la DMZ se quedaron abiertos los siguientes puertos:

21 Protocolo de red para la transferencia de archivos.

22 SSH SSH (Secure Shell).

53 DNS Sistema de Nombres de Dominio.

443 HTTPS/SSL usado para la transferencia segura de páginas web.

8080 al 8099 Redireccionamiento de puertos.

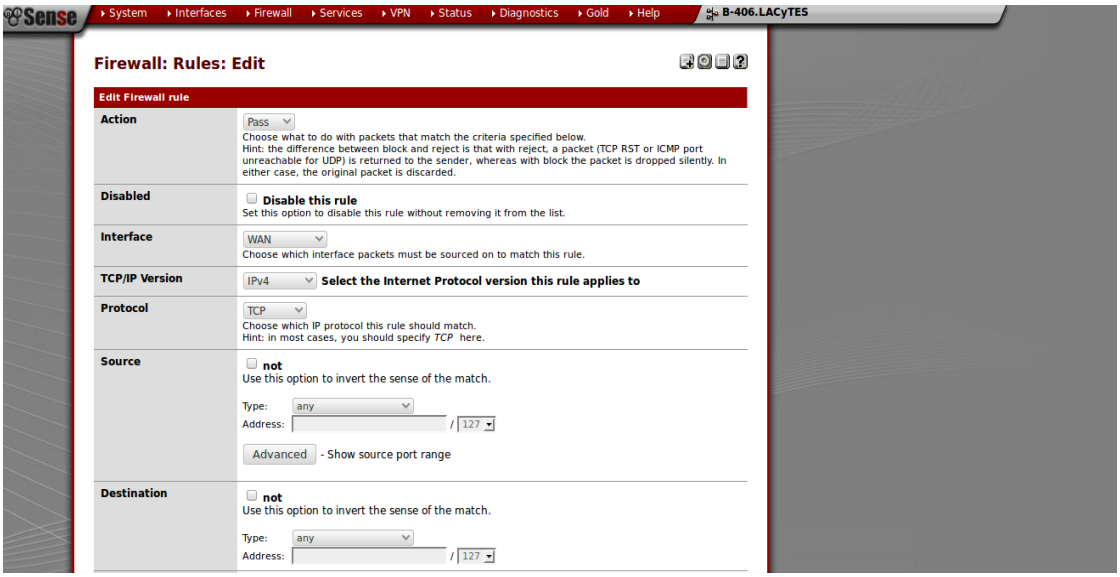
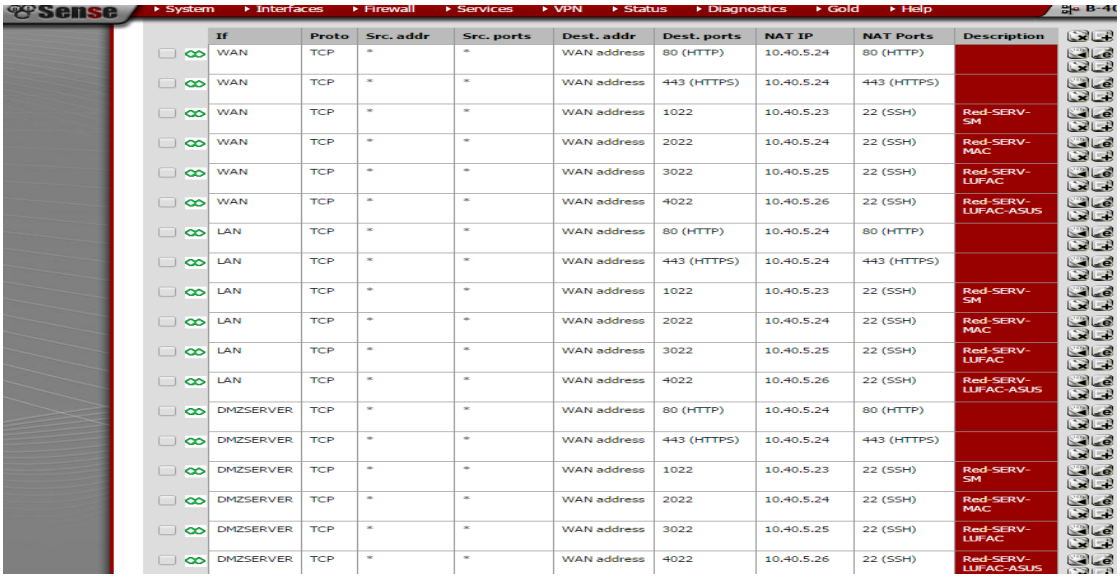


Fig. 2.13 Creación de reglas para permitir o negar el paso de paquetes

Las reglas, que se ejecutan según el orden en que están puestas, es de la primera hacia la última de la lista. Así como el re direccionar el puerto 22 de los servidores para acceso remoto a través de una shell de seguridad es decir, permite que un usuario externo tenga acceso al puerto 22 con una dirección IP de la DMZ desde el exterior a través de Pfsense.



If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN address	80 (HTTP)	10.40.5.24	80 (HTTP)	
WAN	TCP	*	*	WAN address	443 (HTTPS)	10.40.5.24	443 (HTTPS)	
WAN	TCP	*	*	WAN address	1022	10.40.5.23	22 (SSH)	Red-SERV-SM
WAN	TCP	*	*	WAN address	2022	10.40.5.24	22 (SSH)	Red-SERV-MAC
WAN	TCP	*	*	WAN address	3022	10.40.5.25	22 (SSH)	Red-SERV-LUFAC
WAN	TCP	*	*	WAN address	4022	10.40.5.26	22 (SSH)	Red-SERV-LUFAC-ASUS
LAN	TCP	*	*	WAN address	80 (HTTP)	10.40.5.24	80 (HTTP)	
LAN	TCP	*	*	WAN address	443 (HTTPS)	10.40.5.24	443 (HTTPS)	
LAN	TCP	*	*	WAN address	1022	10.40.5.23	22 (SSH)	Red-SERV-SM
LAN	TCP	*	*	WAN address	2022	10.40.5.24	22 (SSH)	Red-SERV-MAC
LAN	TCP	*	*	WAN address	3022	10.40.5.25	22 (SSH)	Red-SERV-LUFAC
LAN	TCP	*	*	WAN address	4022	10.40.5.26	22 (SSH)	Red-SERV-LUFAC-ASUS
DMZSERVER	TCP	*	*	WAN address	80 (HTTP)	10.40.5.24	80 (HTTP)	
DMZSERVER	TCP	*	*	WAN address	443 (HTTPS)	10.40.5.24	443 (HTTPS)	
DMZSERVER	TCP	*	*	WAN address	1022	10.40.5.23	22 (SSH)	Red-SERV-SM
DMZSERVER	TCP	*	*	WAN address	2022	10.40.5.24	22 (SSH)	Red-SERV-MAC
DMZSERVER	TCP	*	*	WAN address	3022	10.40.5.25	22 (SSH)	Red-SERV-LUFAC
DMZSERVER	TCP	*	*	WAN address	4022	10.40.5.26	22 (SSH)	Red-SERV-LUFAC-ASUS

Fig. 2.14 Re direccionamiento de puertos en Pfsense

Por otro lado se implementó el Monitoreo de red para revisar el uso del tráfico en la red buscado problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red u otros dispositivos.

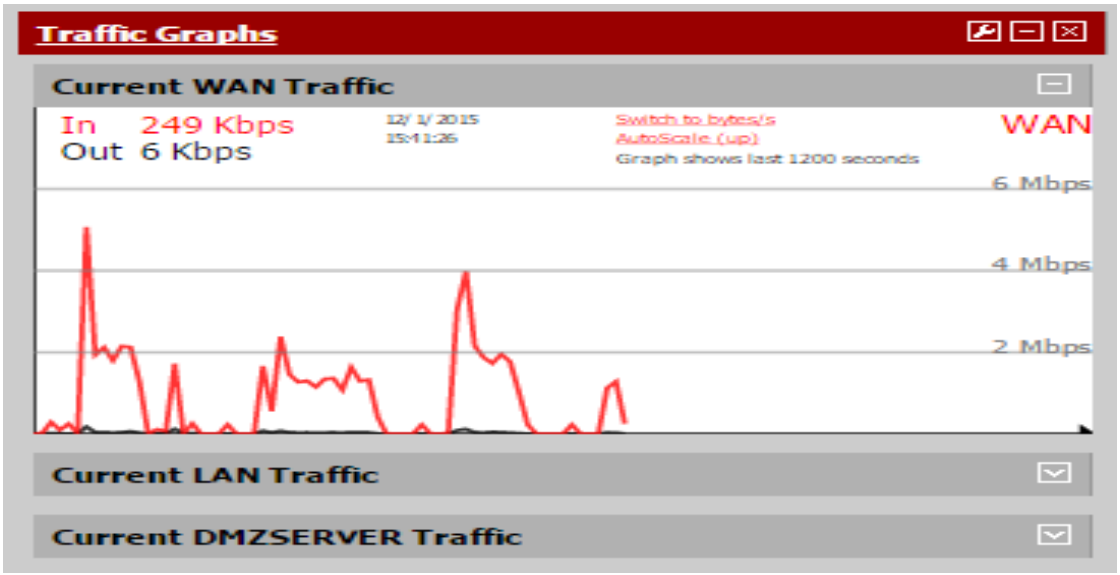


Fig. 2.15 Monitoreo de la red a través de Pfsense

Interface Statistics

	WAN	LAN	DMZSERVER
Packets In	506835	175444	172757
Packets Out	351948	196282	304969
Bytes In	629.37 MB	12.27 MB	14.26 MB
Bytes Out	26.05 MB	250.85 MB	378.30 MB
Errors In	0	0	0
Errors Out	0	0	0
Collisions	0	0	0

Fig. 2.16 Monitoreo de la red a través de Pfsense

Otra medida en la seguridad del cortafuegos importante, es revisar periódicamente los ficheros de "loggins" de los servidores y los del firewall, verificando que no ha habido accesos a horas extrañas, ni de máquinas desconocidas, y de vez en cuando, comprobar que todas las políticas de seguridad que hemos programado siguen activas.

Firewall Logs

Act	Time	IF	Source	Destination
✖	Dec 1 17:25	WAN	172.17.120.158	224.0.0.1
✖	Dec 1 17:27	WAN	172.17.120.158	224.0.0.1
✖	Dec 1 17:30	WAN	172.17.120.158	224.0.0.1
✖	Dec 1 17:32	WAN	172.17.120.158	224.0.0.1
✖	Dec 1 17:34	WAN	172.17.120.158	224.0.0.1

Fig. 2.17 Creación de logs para facilitar la búsqueda de errores

La utilización de backup la cual es una copia de seguridad de la configuración y datos se realiza con la finalidad de tener un medio para recuperarlos en caso de su pérdida o modificación.

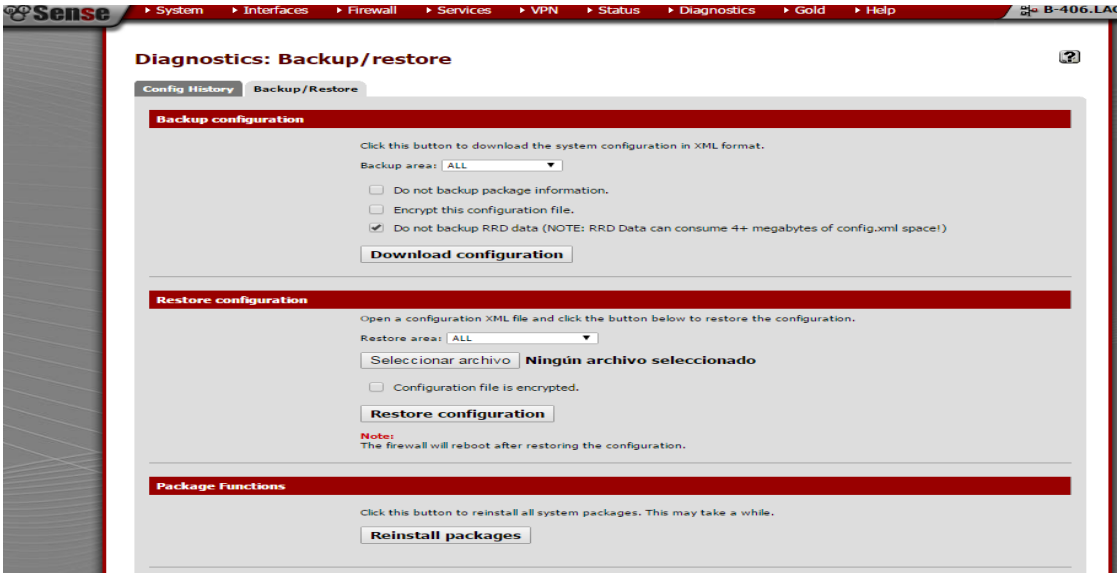


Fig. 2.18 Creación de respaldos del Pfsense

2.4. Resultado de la implementación de Pfsense

Se implementó un cortafuegos con el objetivo de analizar el tráfico desde adentro hacia fuera y viceversa permitiendo sólo el trafico autorizado logrando tener a salvo la información almacenada en los servidores como en los ordenadores. Gracias a la implementación de protocolos editados en Pfsense, se redujo considerablemente las posibilidades de violación de la integridad de la información y de intrusiones de usuarios no deseados en la red y en caso de ser así, también se tomaron medidas para la restauración de la información crítica para este proyecto.

Esto se logró gracias a las siguientes medidas:

- La creación de dos VLANs tanto en Pfsense como en el switch, una para desarrollo e investigación y otra para la DMZ.
- Filtrado MAC en cada VLAN.

- Edición de reglas donde se decidió qué conexiones se permiten y cuáles no, solo dejando abiertos aquellos puertos que sean de utilidad todos los demás se decidieron cerrar.
- Re direccionar el puerto 22 de los servidores para acceso remoto de los servidores en la DMZ.
- Implementación de el monitoreo de red para revisar el uso del tráfico.
- Revisión periódicamente los ficheros de "loggins".
- Utilización de backup.

Esto brindo la protección necesaria a la red, pero en ningún caso se considera suficiente dado que la seguridad en la red abarca más ámbitos y más niveles de trabajo y protección que también se mostraran en siguientes capítulos.

CAPÍTULO 3. PUESTA EN PUNTO DEL SERVIDOR LINUX

El software libre se entiende como la libertad de los usuarios de poder usar un programa para cualquier propósito con la libertad de estudiar cómo funciona el programa y adaptarlo a las necesidades dado que el acceso al código fuente es un privilegio donde también existe la libertad de mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie.

Así, los usuarios tienen el control de sus equipos y no a la inversa, es por eso que se trabajó bajo el esquema Linux con una distribución en base al costo, seguridad, entorno y actualización.
La distribución elegida debe funcionar por muchos años ya que la migración de una a otra puede acarrear costos adicionales.
Según DistroWatch, existen alrededor de 300 distribuciones de Software Libre activas, la mitad de ellas (alrededor de 140) comienzan con Debian y lo cual permite la adaptación a las necesidades de los usuarios, generalmente agregando, modificando o reconstruyendo paquetes y publicando el producto que resulta [8].

3.1 Sistema operativo Debian

Una comparación de varias distribuciones Linux llevó a elegir Debian 8 por varias razones:

Es una distribución comunitaria, con desarrollo asegurado e independientemente de cualquier limitación comercial. Sus objetivos son, por lo tanto, de una naturaleza esencialmente técnica que favorece la calidad general del producto.

De todas las distribuciones comunitarias, es la más significativa desde varias perspectivas: cantidad de contribuyentes, número de paquetes de software disponibles y años de existencia. El tamaño de su comunidad es un testigo innegable de su continuidad.

Algunas de sus características de acuerdo al manual de debían 2011 son:

- . **Sistema de empaquetamiento de software**

  Los archivos de software en las tres versiones anteriores al actual, pueden ser un poco desordenados o al instalar software se puede encontrar que el sistema se colapse debido a conflictos de software. Gracias a dpkg (es el programa base para manejar paquetes Debian en el sistema), el sólido sistema de empaquetamiento de Debian, se encarga de estos asuntos.

- **Cantidad de software**
  Debian viene con más de 37500 paquetes de software disponibles para descargar e instalar y es totalmente libre. Si tiene software propietario que corre bajo GNU/Linux o GNU/FreeBSD, y se puede usar libremente.
- **Código fuente**

  Hay cientos de herramientas y lenguajes de desarrollo, además de millones de líneas de código fuente en el sistema base. Todo el software en la distribución principal es conforme al criterio de las Directrices de Software Libre de Debian (DFSG). Esto significa que se puede usar libremente este código para estudiarlo o para incorporarlo a un nuevo proyecto de

software libre. También hay una buena cantidad de herramientas y código apropiado para el uso en proyectos propietarios.

- **Múltiples arquitecturas y kernels**

  Actualmente Debian soporta un impresionante número de arquitecturas CPU: alpha, amd64, armel, hppa, i386, ia64, mips, mipsel, powerpc, s390, y sparc. También corre con los kernels GNU Hurd y FreeBSD. Además de Linux y con la utilidad debootstrap, es difícil que no se encuentre un dispositivo que no pueda correr Debian.

- **Estabilidad**

  Existen muchos casos de máquinas que trabajan durante más de un año seguido sin reiniciarse. De la misma forma, hay equipos que tan sólo son reiniciados debido a un fallo en el suministro de corriente o a una actualización del hardware.

- **Seguridad del sistema**

  Debian y la comunidad del software libre son muy sensibles a asegurarse de que los arreglos de problemas de seguridad entren en la distribución rápidamente. Normalmente, los paquetes arreglados se hacen disponibles a los pocos días. La disponibilidad del código fuente permite que la seguridad en Debian se evalúe de forma abierta, lo que evita que se implementen modelos de seguridad pobres [9].

- **Software de seguridad**

  Debian 8 tiene paquetes de software que permite enviar correo entre usuarios preservando su privacidad. Además, ssh permite crear conexiones seguras a otras máquinas que tengan ssh instalado.

3.2 Instalación

Para una instalación limpia y segura, se llevó a cabo en tres entapas, la primera etapa fue la configuración de RAID, el cual significa disposición redundante de discos independientes, que es un método de combinación de dos o más discos duros en una unidad lógica cuyo objetivo es obtener un rendimiento óptimo, usando unidades idénticas del mismo modelo y capacidad durante la creación o instalación de un sistema operativo, La segunda etapa será la instalación del sistema operativo minimal en Debían y la tercera etapa será, la instalación y desinstalación de paquetes de software para tener un sistema operativo más seguro y confiable.

Primera etapa configuración de RAID1

En la primera etapa como se mencionó anteriormente se implementó la configuración conocida como RAID 1, debido a que ofrece redundancia en los discos duros. Para utilizarlo, se usan dos discos duros del mismo tamaño (80GB cada uno). De esta manera, todo lo que escriba en uno de ellos será copiado de manera automática y transparente en el segundo. Si alguno de ellos se estropea se pueda recuperar todos los datos recurriendo a la otra unidad, de esta manera, la información del proyecto estará a salvo de posibles daños físicos en el disco duro.

```
root@master:/home/master# cat /etc/debian_version
8.2
root@master:/home/master#    cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdb1[1]
      74217400 blocks super 1.2 [2/1] [_U]

md1 : active (auto-read-only) raid1 sda3[0]
      76104576 blocks super 1.2 [2/1] [U_]

unused devices: <none>
root@master:/home/master#    cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdb1[1]
      74217400 blocks super 1.2 [2/1] [_U]

md1 : active (auto-read-only) raid1 sda3[0]
      76104576 blocks super 1.2 [2/1] [U_]

unused devices: <none>
root@master:/home/master#
```

Fig. 3.1 Comprobación del Raid 1 en el servidor

Segunda Etapa Instalación del Sistema Operativo y paquetería básica

Se instaló Debían 8.2 minimal y este solo contiene la cantidad mínima de software para la instalación, con esto se evitan paquetes innecesarios instalados por default además de controlar los paquetes instalados, así como su configuración.

El equipo en el cual fue montado de muestra en la siguiente figura.

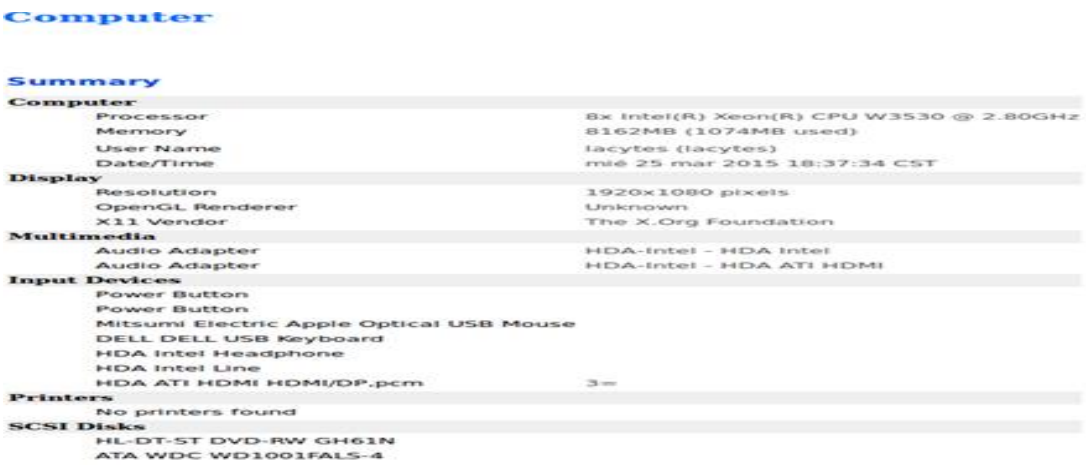


Fig. 3.2 Características del servidor donde se instaló el servidor web para instalación de Joomla

Una vez que se observó las características del servidor en cual fue instalado el sistema operativo se comparó con los requerimientos de sistema operativo de acuerdo al manual de Pfsense 2014 los cuales son:

TIPO	RAM (mínima)	RAM (recomendada)	Disco duro
Sin escritorio	128 megabytes	512 megabytes	2 gigabytes
Con escritorio	256 megabytes	1 gigabyte	10 gigabytes

Fig. 3.3 Requisitos mínimos para la instalación del sistema operativo debían en su versión 8.2.

Comprobación de compatibilidad del servidor e instalación. .

Se descargó una versión ligera de Debian 8 del sitio oficial (https://www.debian.org). El instalador de Debian permite hacer la instalación a través de ficheros de reconfiguración, respondiendo a las preguntas que se formulan durante el proceso de instalación.

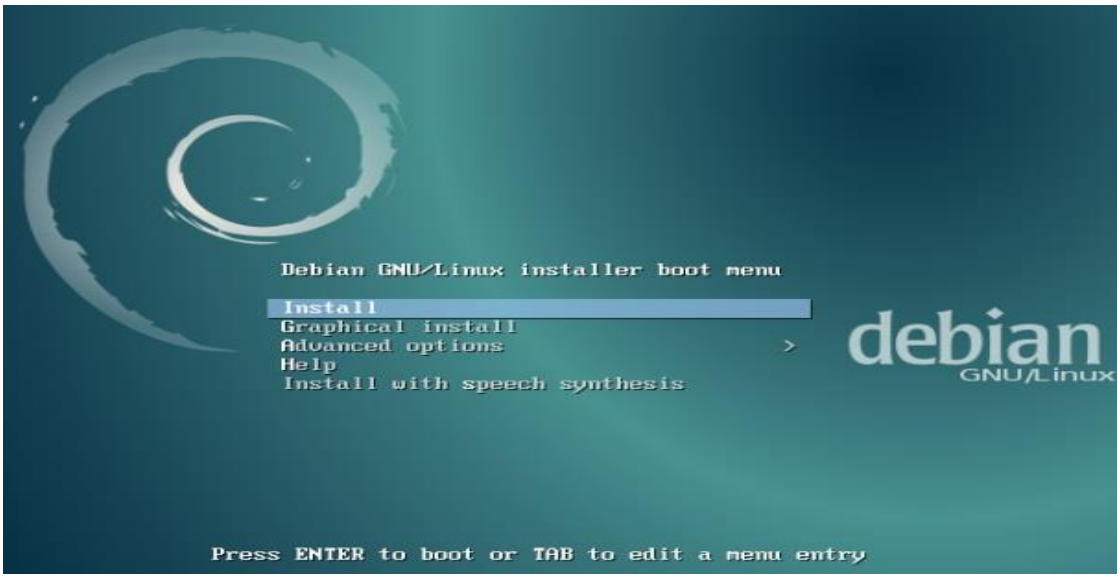


Fig. 3.4 Inicio del instalador de Debian 8.2

Entre las preguntas de instalación del sistema operativo esta asignar usuarios así como las contraseñas, las cuales tiene una gran importancia pues son quien asegura el acceso y control del sistema operativo, así como los servicios que este posea, es por esto que se crearon un nombre de usuario fuerte y contraseña segura lo que permite hacer más seguro el sistema de ataques de fuerza bruta y de diccionario entre otros.

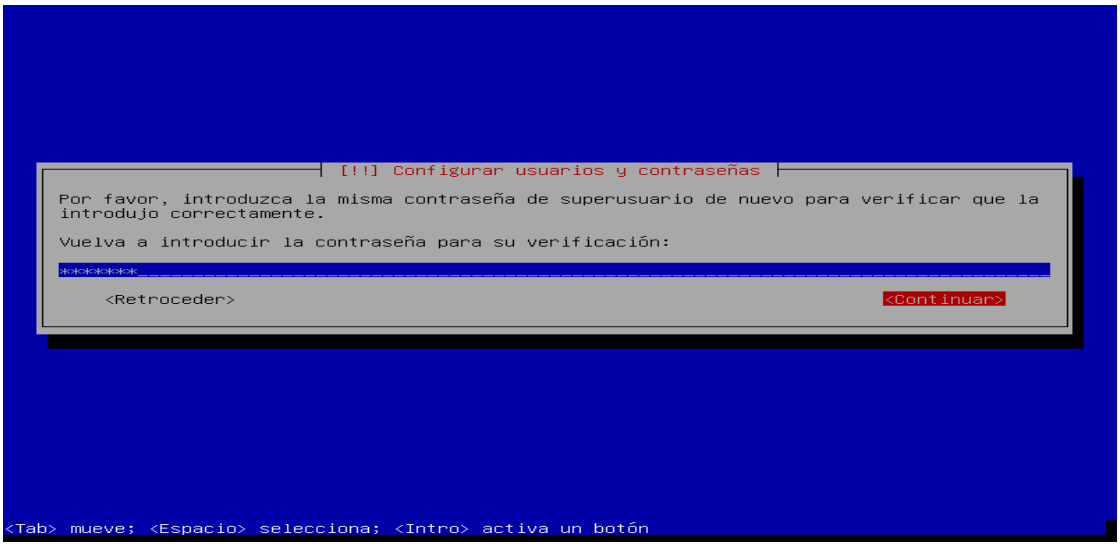


Fig. 3.5 Configuración de usuarios y contraseñas para Joomla

Otra de las opciones que nos permite el instalador de Debian fue cuales servicios y programas deseábamos instalar, en este caso fue lo mínimo para así poder configurar los servicios y programas a las necesidades del proyecto.

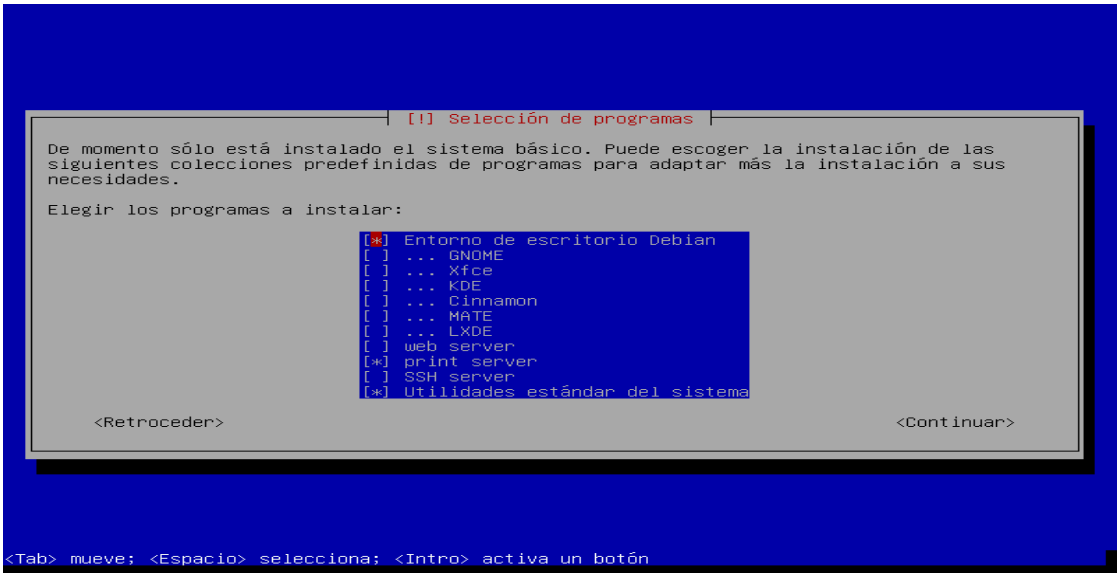


Fig. 3.6 Selección de programas para la instalación de Debian

3.3 Configuración y Seguridad

Una vez que Debian 8 está instalado en el sistema, se realizaron algunas operaciones antes de tenerlo completamente listo y seguro, las acciones que se tomaron en esta etapa fueron las siguientes:

- Actualización del sistema

apt-get update

apt-get upgrade

- Instalación de un servidor web Apache

El Proyecto Apache HTTP Server, desarrolla y mantiene un servidor HTTP de código abierto para sistemas operativos, incluyendo Linux con el objetivo de proporcionar un servidor seguro y extensible

que proporciona servicios HTTP, entre otras características altamente configurables en sincronización con los estándares HTTP actuales [10].

El servidor HTTP se convirtió en el primer servidor web que alojó más de 100 millones de sitios web.

Algunos de los comandos para su instalación fueron:

```
apt-get update
apt-get install apache2 apache2-doc apache2-utils
```

- Limitar el número de procesos en Apache

Esta configuración se realizó para evitar recibir una gran cantidad de peticiones web en el momento en que empiezan a ejecutarse un gran número de procesos Apache y que pueden acabar consumiendo toda la memoria RAM. A partir de ahí, el sistema empieza a tirar del archivo de intercambio por lo que el servidor empezará a responder a una velocidad extremadamente lenta. Si se limita el número de procesos a ejecutar, se evitará esta situación.

Para ello se instaló un módulo para Apache, llamado MPM Prefolk.

```
apt-get install apache2-mpm-prefork
nano /etc/apache2/apache2.conf
```

Una vez finalizada la instalación, se editó el archivo de configuración de Apache como se observa en la figura 3.7.

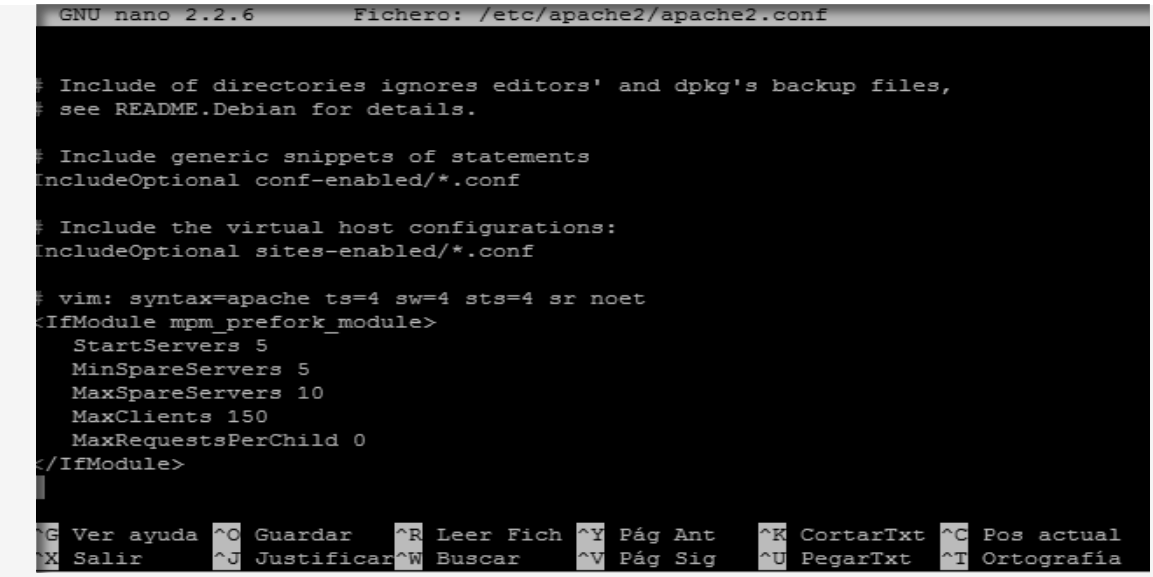


Fig. 3.7 Configuración de módulo MPM Prefolk en Apache.

El significado de cada línea es el siguiente:

StartServers: Número de procesos que de ejecutan al iniciar Apache.

MinSpareServers: Mínima cantidad de procesos que se mantienen en espera. Siempre debe haber procesos en espera ya que de esa forma se acorta el tiempo de acceso de los clientes.

MaxSpareServers: Cantidad máxima de procesos en espera.

MaxClients: Número máximo de procesos que se pueden ejecutar. Este es el valor más importante para controlar el uso de RAM. Para saber cuántos procesos como máximo se deben poder ejecutar, hay que saber cuánto nos ocupa cada uno, algo que depende de varios factores.

MaxRequestsPerChild: es el número de peticiones que atiende cada hilo de ejecución. Si el valor es alto, pueden ocurrir fallos ya que los procesos necesitan reiniciarse periódicamente para limpiar la memoria. Si el número es demasiado bajo el rendimiento se resentirá.

Protección anti ataques DoS

Para esta medida se utilizó el módulo llamado Evasive el cual ayuda a proteger contra DoS, DDoS (Distributed Denial of Service), y los ataques de fuerza bruta en el servidor web Apache. Puede proporcionar una acción evasiva durante los ataques y reportar los abusos a través de servicios de correo electrónico y el registro del sistema [11].

Para su instalación se ejecutó el siguiente comando:

apt-get install libapache2-mod-evasive

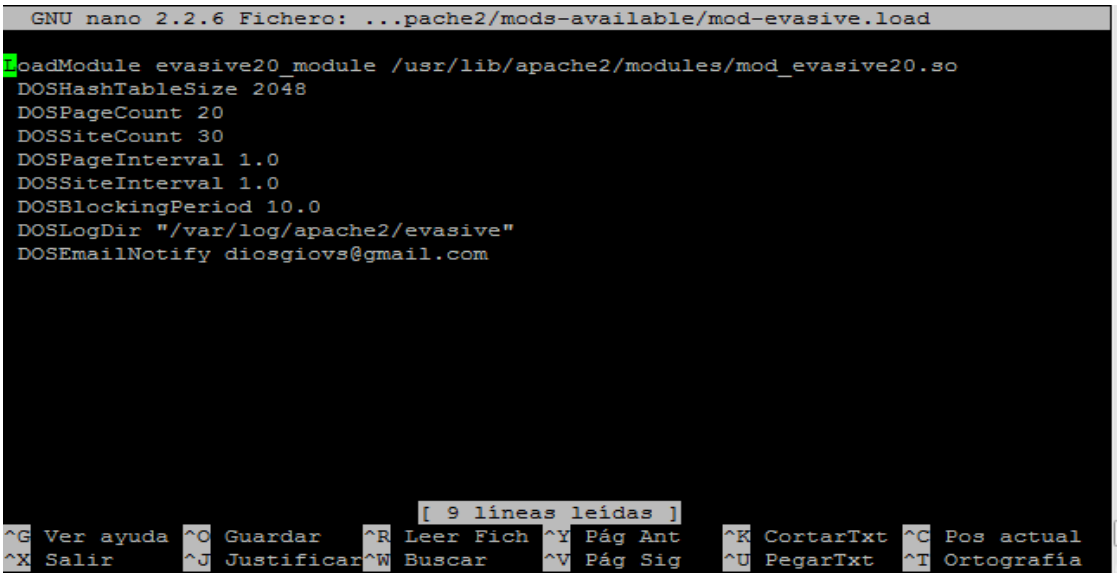


Fig. 3.8 Configuración de módulo Evasive en Apache

Página segura HTTPS con SSL-RSA

HTTPS es la versión segura del protocolo HTTP, consistiendo de una combinación de éste con un mecanismo de transporte SSL y RSA. SSL es un protocolo criptográfico, garantizando así una protección considerable durante la comunicación cliente-servidor mientras que RSA es el sistema

criptográfico. Es ampliamente utilizado en la red mundial web (World Wide Web) para comunicaciones como transacciones bancarias y pago de bienes y servicios entre otras.

Para su instalación se ejecutó el siguiente comando:

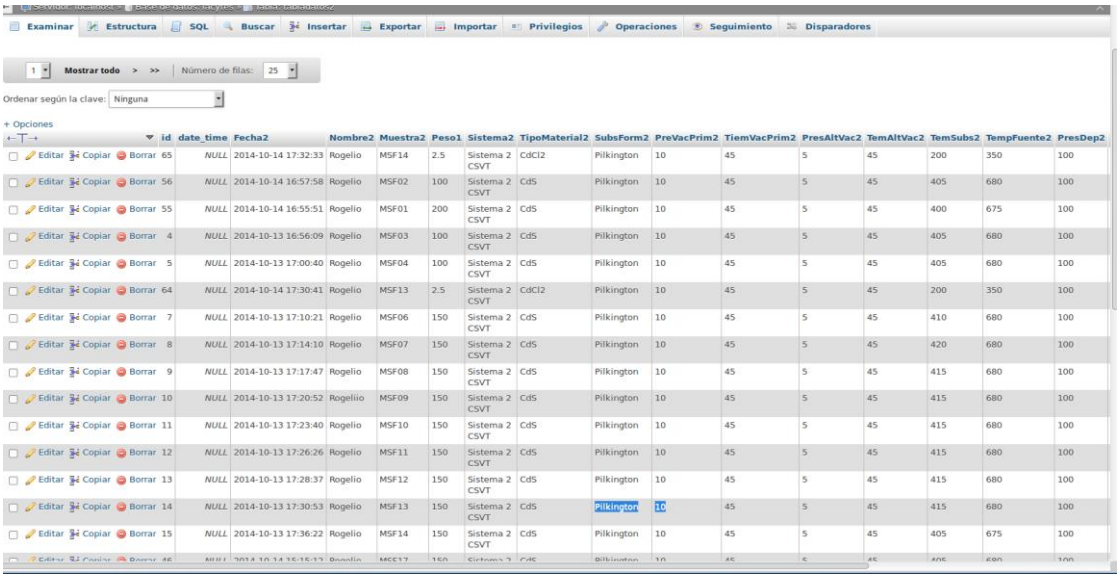
```
# a2enmod ssl
```

En la figura 3.9 muestra como se configuro el cifrado SSL y RSA.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar  1 14:11:36 2016 from 10.40.5.19
lacytes@lacytes:~$ su
Contraseña:
root@lacytes:/home/lacytes# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
root@lacytes:/home/lacytes# a2ensite default-ssla2ensite default-ssl
ERROR: Site default-ssla2ensite does not exist!
Site default-ssl already enabled
root@lacytes:/home/lacytes# /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
root@lacytes:/home/lacytes# openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............................+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

Fig. 3.9 Creación de llaves públicas y privadas para el cifrado en apache

Listo el servidor, se realizó la creación de un usuario y una base de datos en Mysql de la cual se apoyara el sitio web para la captura de datos experimentales y de caracterización en la bitácora del proyecto “Manufactura de módulos fotovoltaicos de CdS/CdTe en áreas de 100 cm^2 y con eficiencias de 8% por la técnica de sublimación y procesos preindustriales asociados”, como se puede observar en la figura siguiente.



	id	date_time	Fecha2	Nombre2	Muestra2	Peso1	Sistema2	TipoMaterial2	SubsForm2	PreVacPrim2	TiemVacPrim2	PresAltVac2	TemAltVac2	TemSubs2	TempFuente2	PresDep2
Editar Copiar Borrar	65	NULL	2014-10-14 17:32:33	Rogelio	MSF14	2.5	Sistema 2 CSVT	CdCl2	Pilkington	10	45	5	45	200	350	100
Editar Copiar Borrar	56	NULL	2014-10-14 16:57:58	Rogelio	MSF02	100	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	405	680	100
Editar Copiar Borrar	55	NULL	2014-10-14 16:55:51	Rogelio	MSF01	200	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	400	675	100
Editar Copiar Borrar	4	NULL	2014-10-13 16:56:09	Rogelio	MSF03	100	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	405	680	100
Editar Copiar Borrar	5	NULL	2014-10-13 17:00:40	Rogelio	MSF04	100	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	405	680	100
Editar Copiar Borrar	64	NULL	2014-10-14 17:30:41	Rogelio	MSF13	2.5	Sistema 2 CSVT	CdCl2	Pilkington	10	45	5	45	200	350	100
Editar Copiar Borrar	7	NULL	2014-10-13 17:10:21	Rogelio	MSF06	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	410	680	100
Editar Copiar Borrar	8	NULL	2014-10-13 17:14:10	Rogelio	MSF07	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	420	680	100
Editar Copiar Borrar	9	NULL	2014-10-13 17:17:47	Rogelio	MSF08	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	10	NULL	2014-10-13 17:20:52	Rogeliio	MSF09	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	11	NULL	2014-10-13 17:23:40	Rogelio	MSF10	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	12	NULL	2014-10-13 17:26:26	Rogelio	MSF11	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	13	NULL	2014-10-13 17:28:37	Rogelio	MSF12	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	14	NULL	2014-10-13 17:30:53	Rogelio	MSF13	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	415	680	100
Editar Copiar Borrar	15	NULL	2014-10-13 17:36:22	Rogelio	MSF14	150	Sistema 2 CSVT	CdS	Pilkington	10	45	5	45	405	675	100

Fig. 3.10 Creación de base de datos en Mysql

La figura 3.10, muestra cómo se gestionaron los primeros parámetros, como son insertar la fecha automáticamente, asignar una etapa del formulario a algún usuario en especial, subir fotos de las muestras obtenidas y no permitir dejar preguntas sin contestar.

CAPÍTULO 4. SERVICIO WEB EN JOOMLA

4.1 Características del software

Joomla es un sistema Gestor de Contenidos gratuito líder en la creación de sitios web, ha tenido éxito desde su aparición hace más de 10 años y existen más de 30 millones de páginas webs creadas con Joomla, tiene más de 10.000 componentes que te permiten ir ampliando las funcionalidades de la página web con opciones como tienda virtual, envío de boletines, foros, galerías de imágenes y un sinfín de posibilidades.

Joomla está basado en PHP y Mysql, por lo que la construcción de aplicaciones se hiso en una plataforma de software libre. El núcleo del framework de Joomla permite construir aplicaciones como:

- Sistemas de control de inventario

  Son los procesos que a través de una organización lleva la administración y almacenamiento de la información y recursos, la clasificando el inventario y la confiabilidad en los recursos, para saber cantidad en existencia así como el tener bien identificados cada uno de ellos.

- Sistemas de reportes de datos

  Es un informe que puede ir acompañado de gráficos, diagramas y tablas de contenido, acerca de los datos cruciales de nuestra información contenida en Joomla.

- Aplicaciones integradoras

  Joomla permite unir varias aplicaciones y artículos en el sitio web para simplificar su visualización e integración con el usuario.

- Catálogos de productos personalizados

  Entre sus funciones permite personalizar los catálogos de los productos mediante aplicaciones así como la integración de instrucciones en HTML, CSS, PHP entre otros lenguajes.

- Sistemas de comercio electrónico

Consiste en la compra y venta de productos y servicios mediante medios electrónicos.

El objetivo de crear la página web del laboratorio LACyTES, es mejorar el tratamiento de la información así como su sistematización y cuantificación de las muestras para la "Manufactura de módulos fotovoltaicos de CdS/CdTe en áreas de 100 cm^2 y con eficiencias de 8% por la técnica de sublimación y procesos preindustriales asociados", donde los investigadores como los estudiantes que están involucrados en dicho proyecto podrán llevar a cabo una bitácora de sus experimentos, lo cual les permitirá cuando deseen consultar dichos resultados y lo podrán hacer desde cualquier lugar. Dentro de esta consulta podrán comparar distintos experimentos, y ver el avance de una muestra.

4.2 Instalación

Una vez vistas las características del gestor de contenidos Joomla se procedió a la instalación como se muestra en el capítulo anterior, se instalaron los requisitos en el servidor que Joomla requiere (PHP, MySQL y Apache), además de la creación de una base de datos necesaria para el sitio, ya lista los requisitos de la instalación se siguieron los sientes pasos:

- Cambio al directorio público de Apache con el comando en Linux cd /var/www/html

- Descarga de Joomla de su sitio oficial mediante el comando

  #wget http://joomlacode.org/gf/download/frsrelease/17609/76804/Joomla_3.3.1-Spanish-Pack_Completo.tar.bz2

- Utilizacion de el comando # tar -xjvf Joomla_3.0.1-Spanish-Pack_Completo.tar.bz2, para descomprimir Joomla.

- Atribución de permisos a la carpeta donde se alojará el sitio mediante el comando chmod -R 755 /var/www/html donde

Los permisos de sistemas Linux se dividen en tres identidades, conocidas como propietario, grupo y otros.

- Propietario (dueño de un archivo o carpeta)
- Grupo (conjunto de privilegiados con acceso a una zona en particular)
- Otros (público en general)
- 5 = Permiso de Lectura y Ejecución (Lectura = 4+ Escritura = 0 + Ejecución = 1)
- 7 = Permiso de Lectura, Escritura y Ejecución (Lectura = 4 + Escritura = 2 + Ejecución = 1)

Finalmente, se ejecuta el instalador ingresando al navegador y escribir: https://localhost,
Donde en ella se abre la pantalla de instalación donde se piden los siguientes datos Nombre del sitio, Descripción, Dirección de Email de administrador, Nombre de usuario del administrador, Contraseña de administrador.

Fig. 4.1 Configuración para la instalación de Joomla

Una vez completada toda la primera etapa de la instalación de Joomla, que mostrada anteriormente, sigue la configuración de la base de datos donde se piden los siguientes parámetros: Tipo de base de datos, Nombre del servidor, Nombre de usuario, Nombre de la base de datos, y Prefijo de tabla.

Fig. 4.2 Conexión de la base de datos en Mysql con Joomla

La última etapa de instalación de Joomla contiene toda la información acerca de la instalación está dividida en 4 grupos: Configuración principal, Configuración de la base de datos, Comprobación de pre-instalación, y Configuración recomendada.

Fig. 4.3 Configuración general de Joomla

4.3 Desarrollo y metodología del sitio web

Una vez montado el gestor de contenidos Joomla, se procedió a montar la platilla personalizándola y eliminando los módulos inútiles, así como la creación de usuarios, instalación de extensiones, y revisión del estado del sitio, esto en la parte de administración que se muestra en la siguiente figura.

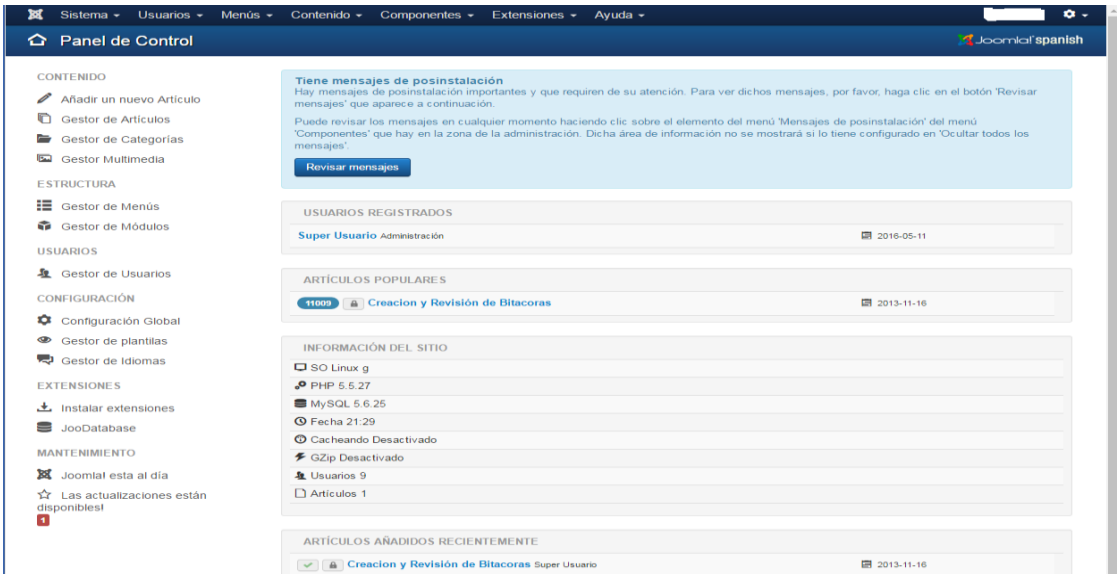


Fig. 4.4 Propiedades generales de Joomla

Se logró el desarrollo del sitio web donde los investigadores y estudiantes que están involucrados en dicho proyecto pueden almacenar y dar seguimiento de sus datos a través de una bitácora electrónica de sus experimentos que les permita consultar resultados desde cualquier lugar (Figura 4.5), para ello se crearon tres niveles de acceso dependiendo del proceso el cual esté involucrado el estudiante o el investigador. El aseso al nivel correspondiente es mediante usuario y contraseña (Figuras 4.6 y 4.7), si el visitante esta fuera de estos tres grupos no podrá asesar a esa información y sólo visualizará la página que se muestra en la imagen anterior. Si la persona pertenece al primer grupo puede entrar a los experimentos y bajo los sistemas CSS y CSVT; el segundo grupo puede asesar a los sistemas RF y DC y el tercer grupo puede entrar a ambos, cabe mencionar que el código utilizado está a disposición en la dirección 172.17.3.51 con el usuario invitado con contraseña Rfvdfg753 en la carpeta docLacytes.

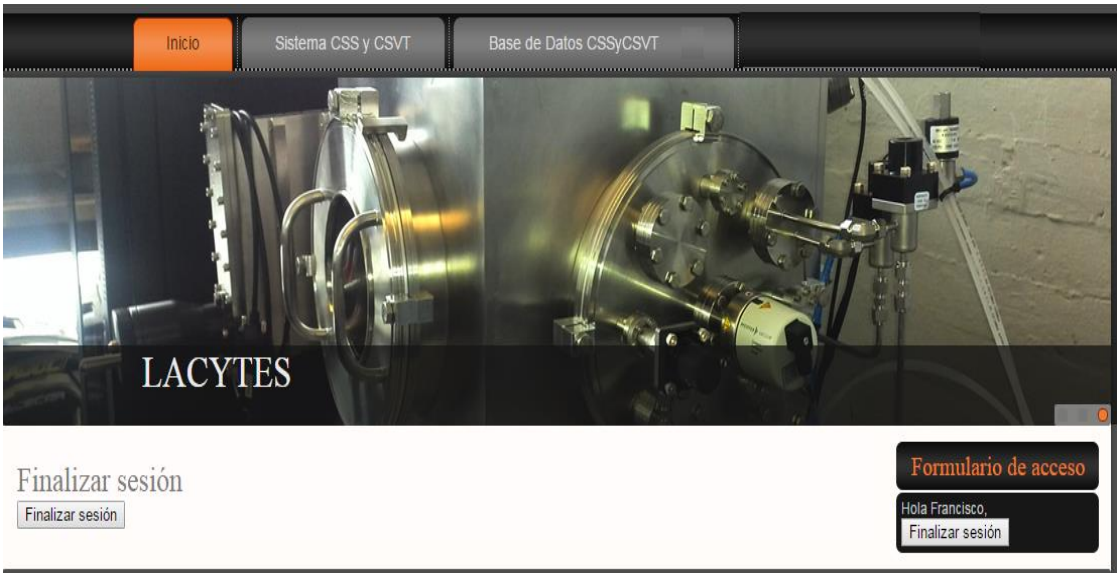


Fig. 4.5 Vista del portal para usuarios del sistema CSS y CSVT

Fig. 4.6 Vista del portal para usuarios del sistema RF Y DC

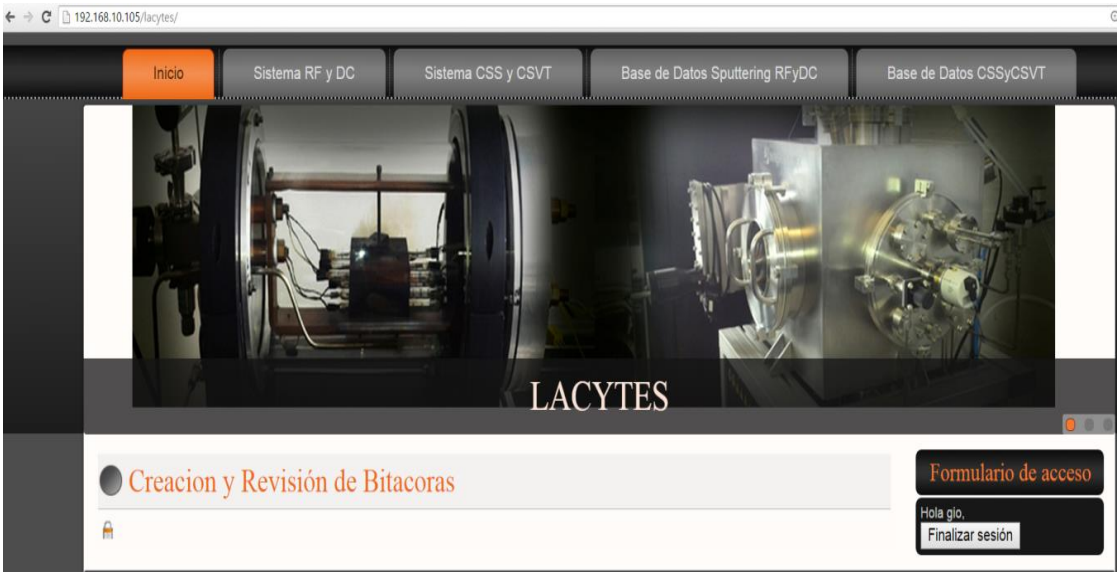


Fig. 4.7 Vista del portal para usuarios con interacción a ambos sistemas

Para los sistemas RF y DC, se elaboró un formulario con el propósito de capturar la información crítica para cada experimento este está vinculado con la base de datos, realizada cuando se instaló mysql, así mismo también se crearon los campos en la base de datos correspondientes a cada pregunta empezando por el nombre y terminando por la imagen de la muestra poniendo la fecha de registro la muestra automáticamente para tener un mayor control así como un marcador, es decir, que es el texto que aparece dentro de un campo de texto antes de que se inserte un contenido. De esta manera, se indica al usuario que inserte en ese campo y con qué parámetros, como se muestra la siguiente figura.

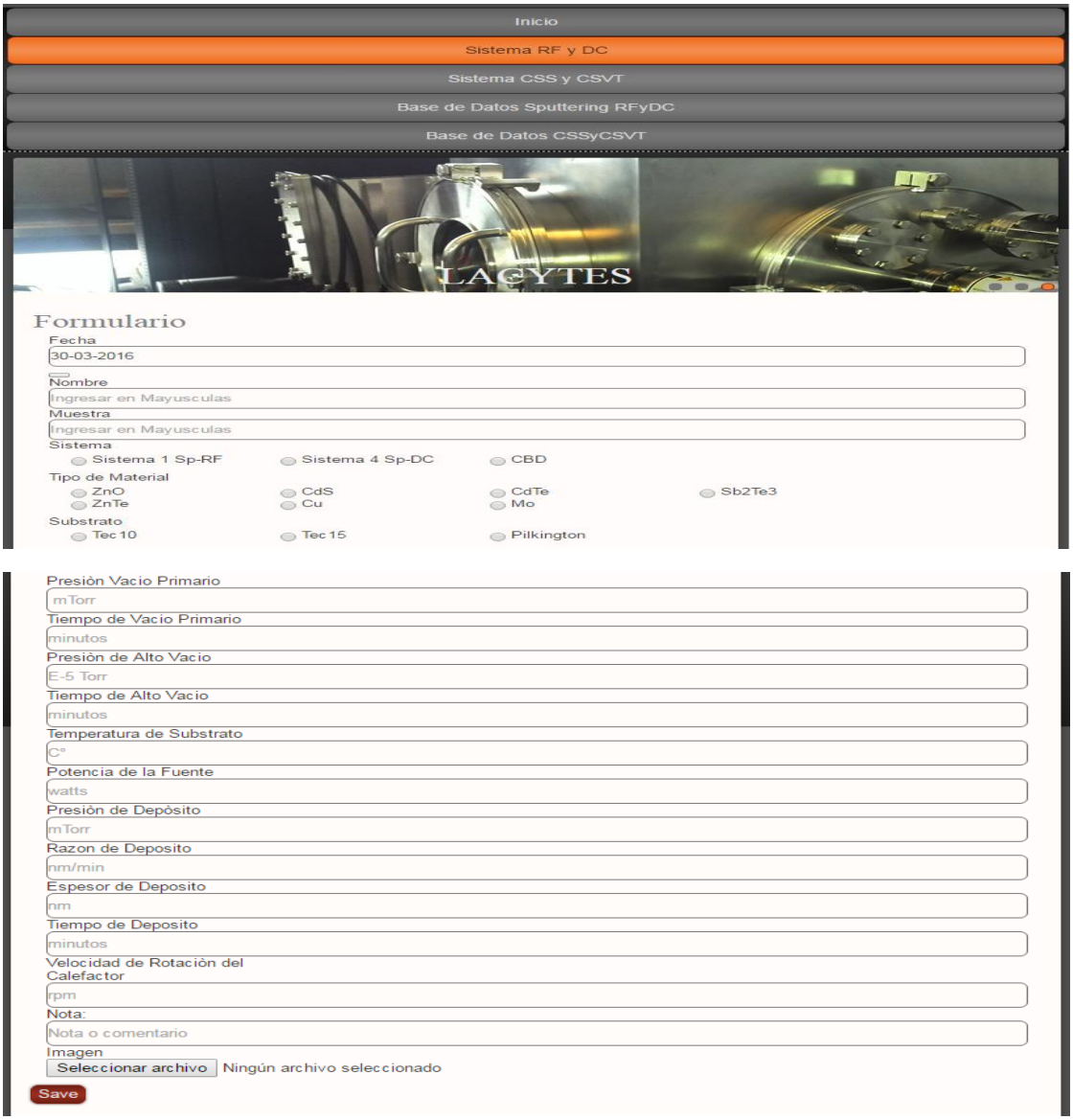


Fig. 4.8 Formulario de registro de bitácoras de experimentos del laboratorio LACyTES

Una vez capturada la muestra y guardada esta, puede consultarse en la pestaña Base de Datos Sputtering RF y DC y/o Base de Datos CSS y CSVT dependiendo de los permisos que el usuario posea y una vez adentro, el usuario posee un buscador de muestras donde podrá buscar una muestra específica, otra característica es una lista de las muestras capturadas con las principales características como una imagen en miniatura de la muestra, fecha de captura, sistema y material.

Cada muestra tiene un hipervínculo donde se muestran todas sus características como se muestran en las siguientes figuras.

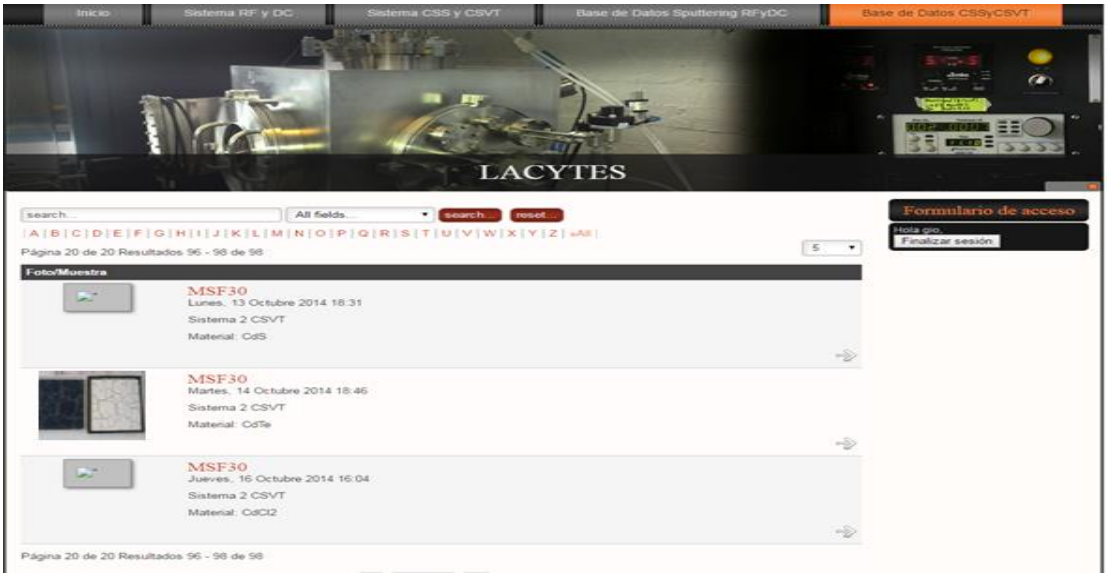


Fig. 4.9 Base de Datos del sistema CSS y CSVT mostrada en Joomla

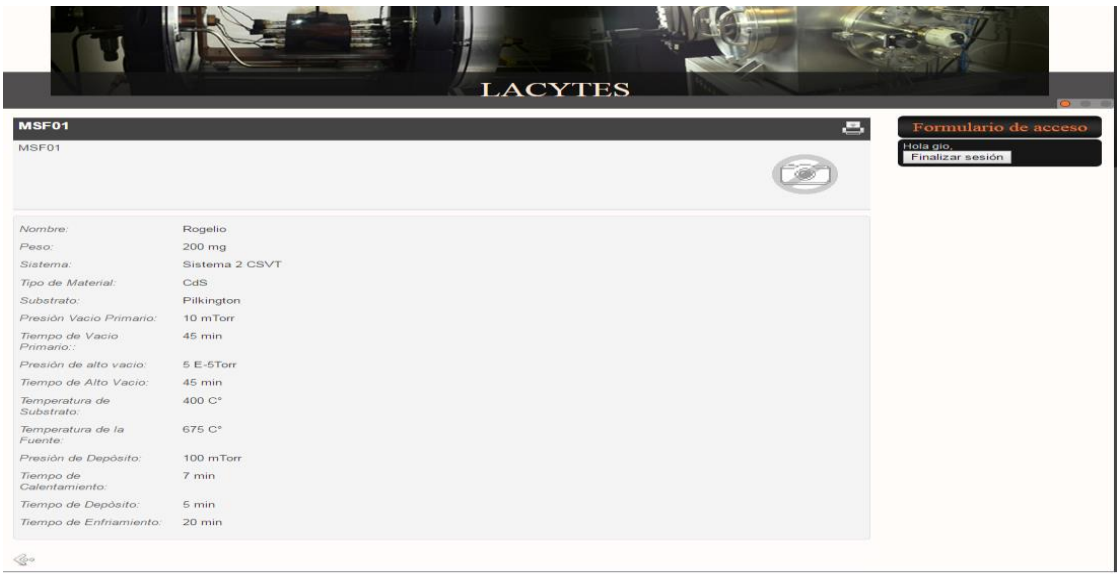


Fig. 4.10 Características de la muestra mostradas en la base de datos

4.4 Medidas de seguridad en Joomla

Un problema de Joomla es que, cualquier usuario puede saber fácilmente si el sitio está desarrollado en Joomla escribiendo la URL para acceder al área de administración (www.sitioweb/administrator).

Esto permite a los que atacan al sistema, obtener un usuario y contraseña para acceder al administrador de Joomla mediante ataques de fuerza bruta, y mediante un script automatizado va probando el acceso a la página web.

La herramienta que se fue jSecure Lite. La cual impide ver la página de acceso a la administración (backend) por el dominio habitual, y solo muestra el formulario de acceso si se usa www.sitioweb.com/?palabra_de_paso. Esta doble validación fortalece la seguridad de Joomla.

Otra medida de seguridad tomada fue la realización de respaldos del sitio web y la base de datos, y realizada periódicamente con la herramienta de Joomla Akeeba Backup, así como la migración a otro servidor fuera del laboratorio para que en el momento en que el equipo llegue a tener algún tipo de daño que lo haga colapsar o se pierda la información, se tenga un respaldo que se podrá poner en operación en segundos.

CAPÍTULO 5. RESULTADOS

Resultados obtenidos

Se obtuvieron satisfactoriamente los objetivos en cada etapa del desarrollo de este proyecto planteados al inicio de esta tesis, algunos de los cuales consistieron en identificar que recursos requieren protección dentro de la red, así como de que amenazas protegernos y en qué grado nos podían afectar, esto nos permitió determinar qué medidas y herramientas implantar para tener un óptimo nivel de seguridad sin perder de vista la relación costo/beneficio.

Estas medidas fueron tomadas en cuenta en cada etapa del proyecto y llevadas a cabo mediante herramientas y protocolos los cuales nos permitieron implementar medidas de prevención, detención y recuperación, que permitieron proteger cada etapa del proyecto.

A continuación se describe los resultados logrados a lo largo de este proyecto en el que se implementaron TIC´s para el laboratorio LACyTES.

En la primera etapa se llevó a cabo la implementación de una red de infraestructura para el laboratorio que provee a los usuarios de la conectividad adecuada tanto a equipos de uso común, como de equipo especializado conectado a la red. La instalación tiene distintos niveles de conectividad que van desde aquellos que se enlazan a red cableada y usuarios de la red inalámbrica para usuarios foráneos y que cuenten con dispositivos móviles, procurando los principios de integridad de la información, así como la disponibilidad y confiabilidad de la misma, como se observa en la Figura 5.1.

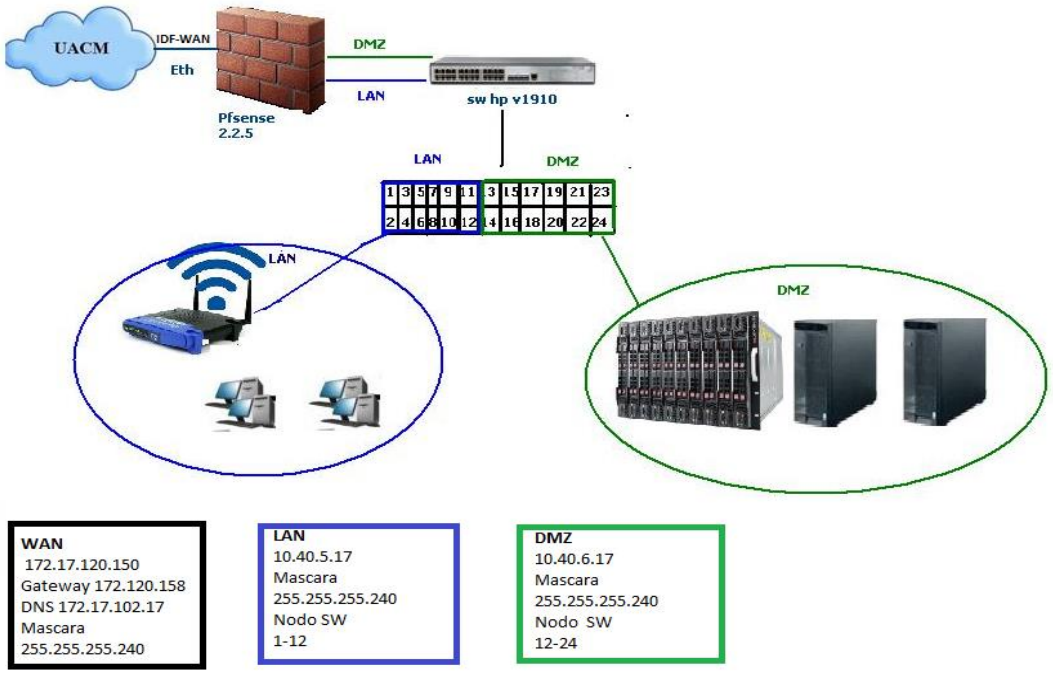


Fig. 5.1 Diagrama de la red del laboratorio LACyTES.

Para lograr este propósito se llevaron a cabo las siguientes acciones, la instalación y configuración de cortafuegos Pfsense, donde es importante destacar la realización de pruebas para comprobar las medias de prevención, detención y recuperación las cuales fueron:

- La creación de dos VLANs en Pfsense, una para desarrollo e investigación donde los equipos en su mayoría cuentan con sistema operativo Windows y otra para la DMZ donde los servidores cuentan con Linux. Para comprobar la configuración de la red se realizaron distintas pruebas, una de estas fue la comprobación de los parámetros de la red mediante el comando ipconfig en Windows (Figura 5.2) e ifconfig en Linux (Figura 5.3) donde se muestran los valores de configuración de red de TCP/IP actuales.

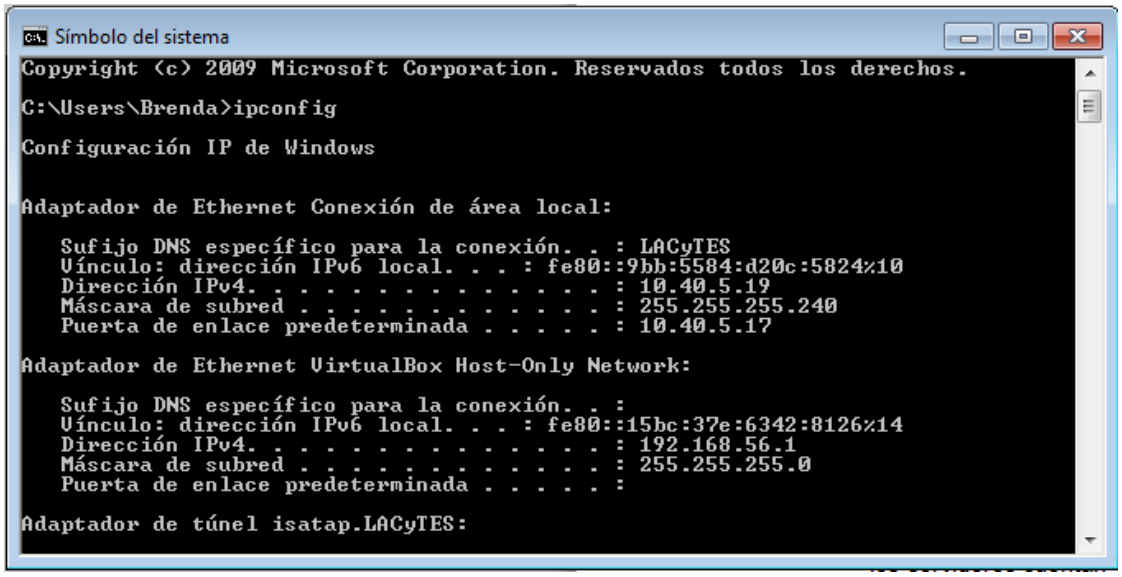


Fig. 5.2 Comando ifconfig donde se observa la configuración la VLAN de investigación donde los equipos poseen Windows

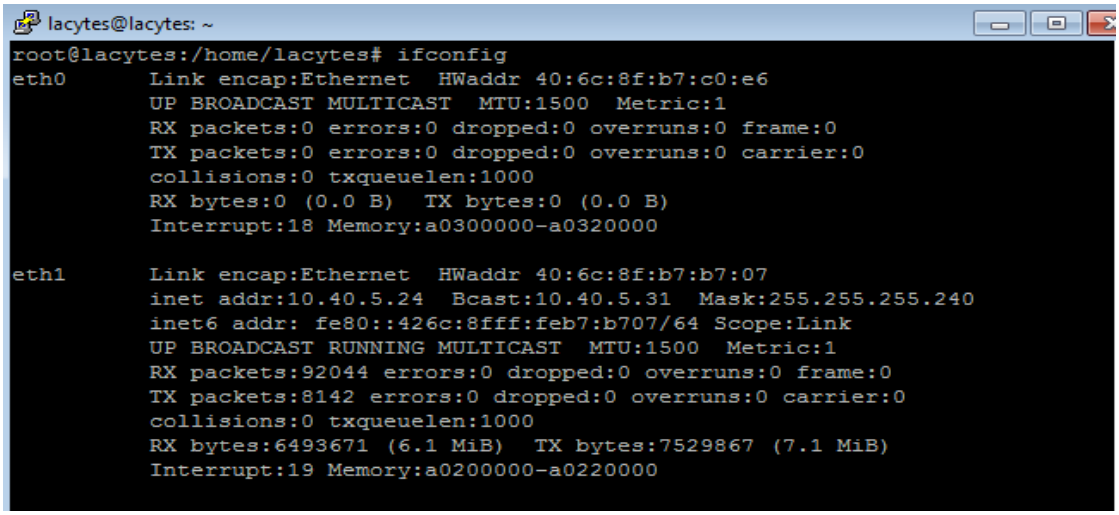


Fig. 5.3 Comando ifconfig en Linux dentro de la DMZ.

- Filtrado MAC en cada VLAN, el cual fue configurado en Pfsense para que el usuario final únicamente conecte su equipo (Figura 5.2) y no tenga que ingresar los valores de la red con esto se disminuyen problemas de ingeniería social.

  ,

- Edición de reglas, donde se decidió qué conexiones se permiten y cuáles puertos dejar abiertos que sean de utilidad. Todos los demás se decidieron cerrar.

- Redireccionamiento del puerto 22 de los servidores para acceso remoto de los servidores en la DMZ.

  Con esta configuración es posible accezar a los servidores por medio de ssh facilitando el trabajo y configuración a distancia de los distintos equipos dentro de la DMZ. Como se puede observar en la siguiente figura, la redirección del puerto 22 de cada servidor es necesaria para poder salir por uno que fue asignado en Pfsense.

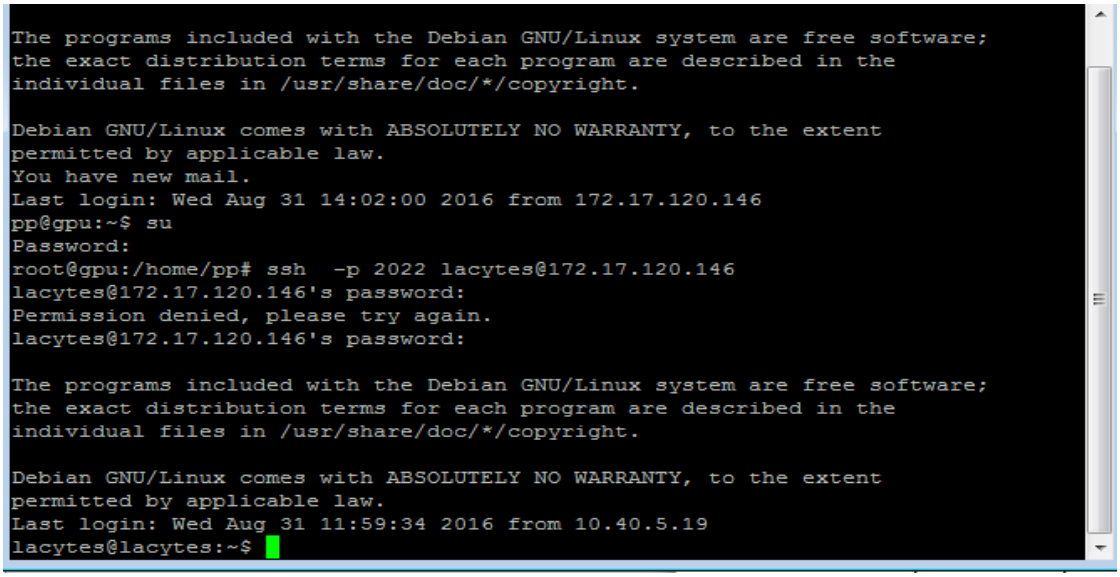


Fig. 5.4 Conexión ssh a la DMZ

- Implementación del Monitoreo de red para revisar el uso del tráfico. Este monitoreo de la red se realiza en búsqueda de usos a comportamientos atípicos en la red y poder tomar medidas para solucionar estos problemas.

- Revisión periódica los ficheros de "loggins", los cuales como ya se menciona anteriormente son los registros, los cuales son de suma utilidad para detectar fallos en la configuración del sistema y corregirlos.

- Creación de respaldos. Esta creación de respaldos es de suma importancia pues dado que una mala configuración o catástrofe natural, se puede recobrar la información y configuración de Pfsense en minutos.

- Configuración del switch hp v1910, El cual es sw configurable gracias a una interfaz web donde también se implementaron dos VLANs asignadas por puerto de esta manera, no solo se controla las VLANs en Pfsense así mismo por el puerto del sw donde son asignados por medio de nodos del sw y etiquetando el cable UTP(Par trenzado no blindado).

-

Otra etapa importante fué la de configurar cinco servidores con debían 8.2 minimal y direccionando el puerto ssh de cada uno. Estos fueron puestos en la DMZ por seguridad, uno de estos se utilizó para la implementación de un sitio web donde los investigadores y estudiantes que esten involucrados en dicho proyecto puedan almacenar y dar seguimiento de sus datos a través de una bitácora electrónica de sus experimentos que les permita consultar los resultados desde cualquier lugar, esto dependiendo de los privilegios con los que cuente el usuario ya que la información desplegada (de acuerdo a los permisos de éste) procura la confidencialidad de la investigación y así como la disponibilidad(Fig. 5.2 Sitio de LACyTES). Sin embargo, para llevar a cabo la mencionada implementación se realizaron una serie de medidas que a continuación se abordarán.

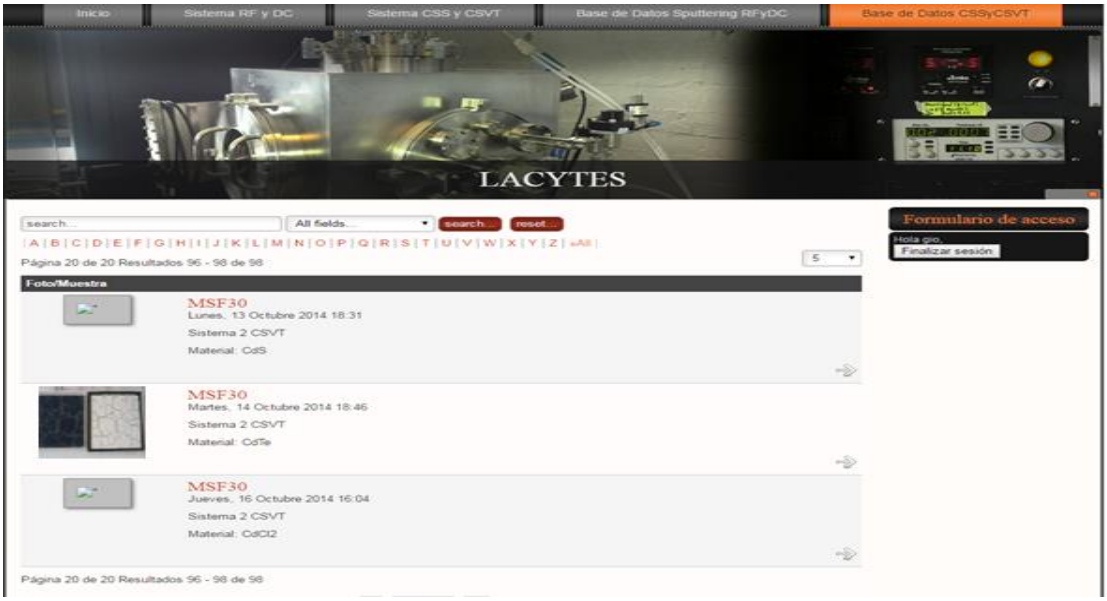


Fig. 5.5 Sitio de LACyTES donde se muestran las bitácoras CSS Y CSVT

Se establecieron parámetros de seguridad dado que en ella se aloja información y datos cruciales sobre los experimentos elaborados en el laboratorio, con estas características se buscaron las herramientas y protocolos que permitieron cumplir los objetivos de forma segura logrando así, la disponibilidad, integridad y confidencialidad. Las medidas implementadas en el servidor fueron las siguientes:

- Implementación de RAID 1
- Instalación de debían 8.2
- Instalación de Apache, donde:

  Se limitaron el número de procesos en Apache

  Se le dio protección anti ataques DoS

  Se implementó el protocolo HTTPS con SSL-RSA

- Instalación de Mysql 5, donde:

  Se creó la de base de datos para muestras

- Instalación de php
- Instalación de phpmyadmin
- Instalación de Joomla, donde:

  Se crearon los formularios para el registro de bitácoras

  Se consultas las bitácoras de forma amigable.

  Se genera el formulario de registro

  Se realiza la creación de usuarios

  Se realiza la creación de niveles de accesibilidad dentro del sitio web

  Se genera el catálogo de las muestras registradas

  Se realiza la creación de respaldos del sitio web

  Se pueda realizar el redireccionamiento de página de acceso a la administración

CAPÍTULO 6. CONCLUSIÓN

En el presente trabajo se menciona los benéficos que se obtuvieron en el laboratorio LACyTES, donde antes de la implementación del sistema de bitácoras electrónicas (desarrolladas en el presente proyecto), se manejaban de una forma engorrosa y lenta, con pérdidas de estos reportes así como de un control mínimo. Gracias a la creación del sitio web, ahora la captura de las bitácoras es más eficiente, rápida y económica debido a la creación de un formulario personalizado para cada investigador o personal involucrado en el desarrollo de los experimentos. Otro de sus beneficios de este trabajo, es que ahora se cuenta con un catálogo vinculado a una base de datos, donde se almacenan todos los formularios, donde a primera vista se encuentran los datos más importantes, dando la opción de conocer más detalles de la muestra, mediante un buscador de muestras. Cabe mencionar que la información de estas bitácoras es confidencial. Así mismo, se trabajó bajo software libre para evitar problemas con licencias, así como una libertad de uso que ofrece, así como y el gran soporte que ofrece sin embargo esto no lo excluye de actualizarlo, así como el actualizarlo cada vez que aparezcan amenazas o vulnerabilidades en el sistema.

Por otro lado, el laboratorio carecía de la estructura para poder dar soporte y mantenimiento al sistema antes mencionado, así que se implementó una red funcional a través de políticas y protocolos, obteniendo una red con VLANs y una DMZ rápida y funcional al servicio de usuarios del laboratorio teniendo en cuenta las diversas necesidades y dando prioridad a la seguridad así como la identificación de la información y equipos utilizados de suma importancia, dentro de la red implementada. En cada nivel de seguridad al igual que en la etapa anterior, todo fue manejado bajo software libre y la seguridad fue implementada de acuerdo al costo beneficio, es decir, se implementó una seguridad que permita a la vez ser confiable y estable.

Otro factor en la construcción de este proyecto, fue la implementación de seguridad en cada nivel de la red, la cual es necesaria para resguardar la integridad de la información y datos que se manejan, sin embargo, esto no garantiza que el sistema sea inmune a amenazas informáticas dado que día a día nuevos programas maliciosos y vulnerabilidades ponen en riesgo el sistema. Además, las malas prácticas por parte del administrador o de los usuarios pueden ocasionar vulnerabilidades, por ello para minimizar el daño se tomaron medidas de prevención, detención, y restauración de sistemas críticos que conlleven a la restauración y/o minimización de daños causados.

Referencias

[1] ISO 27000, «www.iso27000.es,» 29 mayo 2013. [En línea]. Available: http://www.iso27000.es/download/doc_iso27000_all.pdf. [Último acceso: 24 enero 2016].

[2] J. S. Seoane, «http://www.econ.uba.ar/,» 2011. [En línea]. Available: http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/briano/seoane/tp/rivoira/seguridad.htm. [Último acceso: 23 mayo 2014].

[3] Á. Rondán, «redseguridad.com,» 15 Agosto 2015. [En línea]. Available: http://www.redseguridad.com/opinion/articulos/seguridad-en-servidores-web-la-importancia-de-tener-un-sistema-seguro.

[4] C. Solis, «segu info,» 2015. [En línea]. Available: http://blog.segu-info.com.ar/2012/08/5-de-fallas-de-seguridad-de-tu-sitio.html?m=0. [Último acceso: 14 enero 2015].

[5] A. Aguilar Domínguez, «Coodirnación de Seguridad de la Información,» 14 Agosto 2015. [En línea]. Available: www.seguridad.unam.mx/documento/?id=35. [Último acceso: 27 agosto 2015].

[6] welivesecurity, «welivesecurity,» 14 Mayo 2015. [En línea]. Available: www,welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf. [Último acceso: 28 Mayo 2015].

[7] sharpmind software, «sharpmind software,» 13 agosto 2014. [En línea]. Available: http://sharpmindsoftware.com/los-diez-10-tipos-de-vulnerabilidades-de-bases-de-datos-mas-comunes.b.aspx. [Último acceso: 14 septiembre 10].

[8] S. Zacchiroli, «debian-handbook.info,» 24 Octubre 2015. [En línea]. Available: https://debian-handbook.info/browse/es-ES/stable/preface.html.

[9] Manual de Debian, 31 Diciembre 2011. [En línea]. Available: https://www.debian.org/intro/why_debian.es.html.

[10] A. S. F. «Apache HTTP Server for Windows,» 24 Julio 2014. [En línea]. Available: http://descargar.cnet.com/Apache-HTTP-Server-for-Windows/3000-2247_4-10803652.html.

[11] J. Román Mantinez, «emezeta,» 29 Julio 2014. [En línea]. Available: http://www.emezeta.com/articulos/mod-evasive-evitando-denegacion-servicio-distribuida.

[12] eset, «support.eset.com,» 2015 junio 2015. [En línea]. Available: http://support.eset.com/kb186/?viewlocale=es_ES. [Último acceso: 23 mayo 2015].

ANEXOS

Anexo 1. Puertos y sus funciónes

- 1 : TCP Port Service Multiplexer (TCPMUX)
- 5 : Remote Job Entry (RJE)
- 7 : Protocolo Echo (Responde con eco a llamadas remotas)
- 9 : Protocolo Discard (Elimina cualquier dato que recibe)
- 13 : Daytime (Fecha y hora actuales)
- 17 : Quote of the Day (Cita del Día)
- 18 : Message Send Protocol (MSP)
- 19 : Protocolo Chargen, Generador de caractéres
- 20 : FTP — Datos
- 21 : FTP — Control
- 22 : SSH, scp, SFTP – Remote Login Protocol
- 23 : Telnet
- 25 : Simple Mail Transfer Protocol (SMTP)
- 29 : MSG ICP
- 37 : Time
- 42 : Host Name Server (Nameserv)
- 43 : WhoIs
- 49 : Login Host Protocol (Login)
- 53 : Domain Name System (DNS)
- 66 : Oracle SQLNet
- 67 : BOOTP (BootStrap Protocol) (Server), también usado por DHCP
- 68 : BOOTP (BootStrap Protocol) (Client), también usado por DHCP
- 69 : Trivial File Transfer Protocol (TFTP)
- 70 : Gopher Services
- 79 : Finger
- 80 : HTTP
- 88 : Agente de autenticación Kerberos
- 103 : X.400 Standard
- 107 : Remote Telnet Service
- 108 : SNA Gateway Access Server
- 109 : POP2
- 110 : POP3
- 115 : Simple File Transfer Protocol (SFTP)
- 118 : SQL Services
- 119 : Newsgroup (NNTP)
- 123 : NTP

- 137 : NetBIOS Name Service
- 138 : NetBIOS Datagram Service
- 139 : NetBIOS Session Service
- 143 : Internet Message Access Protocol (IMAP)
- 156 : SQL Server
- 161 : SNMP
- 162 : SNMP-trap
- 177 : XDMCP (Protocolo de gestión de displays en X11)
- 179 : Border Gateway Protocol (BGP)
- 190 : Gateway Access Control Protocol (GACP)
- 194 : Internet Relay Chat (IRC)
- 197 : Directory Location Service (DLS)
- 209 : Quick Mail Protocol
- 217 : dBASE Unix
- 389 : Lightweight Directory Access Protocol (LDAP)
- 396 : Novell Netware over IP
- 443 : HTTPS
- 444 : Simple Network Paging Protocol (SNPP)
- 445 : Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
- 458 : Apple QuickTime
- 500 : IPSec ISAKMP, Autoridad de Seguridad Local
- 512 : exec
- 513 : login
- 514 : syslog usado para logs del sistema
- 515 : Printer
- 520 : RIP
- 522 : Netmeeting
- 531 : Conference
- 546 : DHCP Client
- 547 : DHCP Server
- 563 : SNEWS
- 569 : MSN
- 631 : CUPS: sistema de impresión de Unix
- 666 : identificación de Doom para jugar sobre TCP
- 992 : Telnet SSL
- 993 : IMAP4 SSL
- 995 : POP3 SSL
- 1080 : Socks Proxy
- 1352 : IBM Lotus Notes/Domino RCP
- 1433 : Microsoft-SQL-Server
- 1434 : Microsoft-SQL-Monitor
- 1494 : Citrix MetaFrame Cliente ICA
- 1512 : WINS
- 1521 : Oracle listener
- 1701 : Enrutamiento y Acceso Remoto para VPN con L2TP
- 1723 : Enrutamiento y Acceso Remoto para VPN con PPTP
- 1761 : Novell Zenworks Remote Control utility
- 1863 : MSN Messenger

- 2049 : NFS
- 2082 : CPanel
- 2086 : WHM (Web Host Manager)
- 2427 : Cisco MGCP
- 3000 : Calista IP phone (saliente)
- 3030 : NetPanzer
- 3128 : Squid Proxy
- 3306 : MySQL
- 3389 : Microsoft Terminal Server
- 3396 : Novell agente de impresión NDPS
- 3690 : SubVersion
- 4099 : AIM Talk
- 4662 : eMule
- 4672 : eMule
- 4899 : RAdmin
- 5000 : UPNP (Universal plug-and-play)
- 5060 : SIP (Session Initiation Protocol)
- 5190 : Calista IP phone (entrante)
- 5222 : XMPP/Jabber: conexión de cliente
- 5223 : XMPP/Jabber: puerto por defecto para conexiones de cliente SSL
- 5269 : XMPP/Jabber: conexión de servidor
- 5432 : PostgreSQL
- 5500 : VNC (Virtual Network Computing)
- 5517 : Setiqueue proyecto SETI@Home
- 5631 : pcAnyWhere (host)
- 5632 : pcAnyWhere (host)
- 5400 : VNC (Virtual Network Computing)
- 5600 : VNC (Virtual Network Computing)
- 5700 : VNC (Virtual Network Computing)
- 5800 : VNC (Virtual Network Computing)
- 5900 : VNC (Virtual Network Computing)
- 6000 : X11 usado para X-windows
- 6112 : Blizzard Entertainment
- 6129 : Dameware: Software conexión remota
- 6346 : Gnutella
- 6347 : Gnutella
- 6348 : Gnutella
- 6349 : Gnutella
- 6350 : Gnutella
- 6355 : Gnutella
- 6667 : IRC
- 6881 : BitTorrent: puerto por defecto
- 6891-6900 : MSN Messenger (archivos)
- 6901 : MSN Messenger (voz)
- 6969 : BitTorrent: puerto de tracker
- 7100 : Servidor de Fuentes X11
- 8000 : Shoutcast
- 8080 : HTTP alternativo al puerto 80. También Tomcat default
- 8118 : privoxy
- 8291 : routers Microtik
- 9009 : Pichat peer-to-peer chat server
- 9898 : Dabber (troyano)
- 10000 : Webmin (Administración remota web)
- 12345 : Netbus (troyano)
- 19226 : Puerto de comunicaciones de Panda Agent

- 20000-20019 : ICQ
- 31337 : Back Orifice (troyanos)
- 28800-29000 : MSN Game Zone