PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TÍTULO:
"CONFIGURACIÓN DEL FIREWALL DE APLICACIONES WEB MODSECURITY PARA PREVENIR DIVERSOS ATAQUES HACIA APLICACIONES WEB ALOJADOS EN SERVIDORES OPEN SOURCE"

LINEA DE INVESTIGACIÓN:
REDES Y TELECOMUNICACIÓN

AUTOR:
CABEZAS CEDEÑO NATALIE KARINE

ASESOR:
Mgt. GUSTAVO CHANGO

FECHA: Esmeraldas, 2020

TRIBUNAL DE GRADUACIÓN

Trabajo de tesis aprobado luego de haber cumplido los requisitos exigidos por el reglamento de Grado de la PUCESE previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

ASESOR	Mgt. Gustavo Chango Sailema
PRIMER LECTOR	Mgt. Juan Casierra Cavada
SEGUNDO LECTOR	Mgt. Marc Grob
DIRECTOR DE CARRERA	Mgt. Susana Patiño Rosado

AUTORÍA

Yo, **NATALIE KARINE CABEZAS CEDEÑO**, portadora de la cédula de identidad No. 0802557454, confirmo que las ilustraciones, tablas y los resultados obtenidos en la investigación que presento como tesis de grado, previo a la obtención del título de "Ingeniero en Sistemas y computación", son absolutamente originales y personales.

Al mismo tiempo, declaro que todo el contenido incluyendo resultados y conclusiones son de exclusiva responsabilidad académica y legal.

CABEZAS CEDEÑO NATALIE KARINE
C.I 0802557454

DEDICATORIA

Este trabajo de investigación se lo dedico a Dios por iluminar mi mente en cada paso de este proceso llamado vida.

A mi papá Andrés Cabezas por el apoyo incondicional.

A mi mamá Susana Cedeño por ser pilar fundamental en mi vida, darme las palabras de aliento para levantarme cuando he caído.

A mis hermanas y mis pequeños sobrinos por llenar mis días de alegría y estar cuando más los necesito.

A mis abuelitos, tios y demás familiares por siempre confiar en mí.

Natalie Cabezas

AGRADECIMIENTO

Agradecida eternamente con Dios por permitirme culminar una etapa más en vida.

A mi familia por ser parte de este proceso y darme el apoyo que he necesitado en el transcurso de mi vida universitaria.

Agradezco a mis maestros que han tenido el don de la enseñanza y por la contribución a mi formación académica.

A mis compañeros y amigos con los que he compartido este proceso que hoy culmina.

Natalie Cabezas

RESUMEN

La presente investigación fue desarrollada con el objetivo de fortalecer la seguridad y reducir las vulnerabilidades en servidores web, usando el Firewall de aplicaciones web por sus siglas en inglés (WAF) de código abierto Modsecurity.

El ambiente de prueba se realizó configurando un servidor con Centos e implementando la tecnología de contenedores “docker”, el cual permitió tener dos escenarios, dentro del cual fue instalado el servidor web apache realizando el levantamiento de una página web, haciendo uso de la imagen con el CMS (Sistema de gestión de contenidos), Wordpress, para las pruebas se establecieron dos escenarios el primero no contaba con ningun tipo de seguridad como son certificado SSL, Modsecurity, mientras que el segundo se implementó niveles de seguridad.

En ambos escenarios se ejecutaron ataques para realizar las comparaciones entre los dos entornos, se llevó acabo dos de los ataques más comunes, DoS y DdoS.

Con la ejecución de los ataques en ambos escenarios se pudo obtener que el servidor web con el protocolo de transferencia de hipertexto (HTTP) fue más fáciles de vulnerar a diferencia del escenario que contaba con el protocolo seguro de transferencia de hipertexto (HTTPS) y WAF el cual no pudo ser vulnerado.

Palabras claves: WAF, Modsecurity, Seguridad, HTTP, HTTPS.

ABSTRACT

This research was developed with the aim of strengthening security and reducing vulnerabilities in web servers, using the open source Modsecurity Web Application Firewall (WAF).

The test environment was done by configuring a server with Centos and implementing the technology of "docker" containers, which allowed for two scenarios, within which the Apache web server was installed by lifting a web page, using the image with the CMS (Content Management System), Wordpress, for the tests two scenarios were established the first did not have any security such as SSL certificate, Modsecurity, while the second implemented security levels.

In both scenarios, attacks were executed to make comparisons between the two environments. Two of the most common attacks were carried out, DoS and DdoS.

With the execution of attacks in both scenarios, it was possible to obtain that the web server with the hypertext transfer protocol (HTTP) was easier to compromise, unlike the scenario with the secure hypertext transfer protocol (HTTPS) and WAF, which could not be compromised.

Keywords: WAF, Modsecurity, Security, HTTP, HTTPS.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

PRESENTACIÓN DE LA INVESTIGACIÓN

El actual trabajo de investigación está focalizado en la configuración del firewall para aminorar ataques, haciendo énfasis en los factores vitales para el resguardo de un servidor web como son la infraestructura, protocolos de seguridad, certificados válidos y actualizados.

En el estudio de dicha problemática es requerido indicar que las razones que llevan a la vulnerabilidad son consecuentes a la existencia de ataques, los cuales suceden debido a la incorrecta configuración del firewall, además de la falta de posesión de certificados.

Para obtener la categoría en la que se encuentra el sitio web se hizo uso de la herramienta tecnológica online SSL LABS, este instrumento tecnológico automatiza el proceso de verificar suites de cifrado y certificados digitales lo cual es significativo ya que permite obtener el nivel de seguridad con el que cuenta el sitio.

La determinación, investigación y gestionamiento de las amenazas y vulnerabilidades en los sitios web, permitirá aumentar la seguridad, afianzando la experiencia de los usuarios en un área en la cual se sientan seguros de compartir su información, además de prevenir ciberataques.

La metodología aplicada es bibliográfica y experimental, mediante la investigación bibliográfica se obtuvo la información teórica, que fue organizada permitiendo obtener valor crítico de las investigaciones previas.

El proyecto de investigación está constituida por tres capítulos, expuesto de forma breve a continuación:

Capítulo I: Basado en el marco teórico, en el cual se desarrollan los conceptos primordiales y precisos de la investigación, considerando los antecedentes de estudios

efectuados como base, y sus diferentes definiciones elementales, amenazas y firewall de aplicaciones web.

Capítulo II: Detalla las metodologías con las que se ejecutó el desarrollo de la investigación, mostrando minuciosamente factores relevantes y los instrumentos que fueron usados para el desarrollo metodológico.

Capítulo III: Expone los resultados adquiridos después de haber realizado la parte experimental de la investigación especificando las bases teóricas que se presentaron en el capìtulo I y II.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen sitios web que no cuentan con la seguridad que se requiere por este motivo está sujeto a recibir ataques por personal mal intencionado con el fin de echar a perder el sistema o sustraer información.

Sin embargo, en los últimos años ha incrementado herramientas tecnlógicas para la seguridad en la web, siendo el caso del WAF modsecurity, para implementarlo se necesita las configuraciones, los certificados vigentes para el buen funcionamiento y poder mitigar los ataques al servidor web.

JUSTIFICACIÓN

La presente investigación pretende sugrerir a la “Pontificia Universidad Católica del Ecuador Sede Esmeraldas” una propuesta de configuración de un firewall para mitigar ataques en su servidor web.

En la actualidad las aplicaciones web se han convertido en las principales prestadoras de servicio a través del internet, esto se debe a la evolución de la tecnología que permite tener información de una entidad lo cual es significativo ya que también proporciona realizar pagos al tener un sitio de ventas.

Por tal motivo las aplicaciones web al no contar con las configuraciones y los respectivos módulos de seguridad están sujetos a cualquier ataque, debido a esto se analizó y corrigió los errores.

Bo Li y Guiqin Yuan en su investigación explican la detección de anomalías en la web esto es importante porque permite el reconocimiento de errores, y les permitió dar resultado a su objetivo que era encontrar desviaciones del comportamiento normal que ocurrieron en su sistema la mayor parte del tiempo, explicando que pocos estudios se interesan sobre las anomalías causada por inyección SQL [1].

Jisa David y Ciza Thomas se refieren a las aplicaciones de internet y hacen relevancia a que contribuyen a mejorar el uso del sistema, sin embargo los sistemas son vulnerables a gran cantidad de ataques, uno de ellos la denegación de servicios distribuida (DoS) [2].

Otro estudio realizado por Das Debashisy Utpal Sharma declara con respecto a su investigación, cada vez que las aplicaciones web ejecutan sentencias dinámicas SQL puede sufrir ataques de inyección [3], lo que significa que la información de los usuarios o de las entidades quedan vulnerables.

Esta propuesta permitirá una experiencia segura y beneficiará a todas las organizaciones que manejen sitios web como fuente de interacción con clientes y usuarios.

OBJETIVOS

GENERAL

Fortalecer la seguridad para reducir las vulnerabilidades en un servidor web mediante la configuración de un firewall.

ESPECÍFICOS

- Configurar el firewall de aplicaciones web (WAF) Mod Security para reducir ataques al servidor
- Aplicar Fail2ban como estrategia de seguridad para mitigar ataques DOS
- Implementación de Mod Evasive para evitar la denegación de servicio distribuido (DDOS)

CAPÍTULO I: MARCO TEÓRICO

1.1 ANTECEDENTES

El firewall es una tecnología que apareció a finales de 1980 justo después de la existencia de los routers. Aunque su existencia era antigua tuvo gran impacto dentro de las pequeñas y medianas empresas hasta el año 2013, en los dos siguientes años existieron problemas de seguridad. Existió vulnerabilidad crítica en plataformas como Drupal y en el plugin RevSlider para WordPress [4].

En la investigación realizada por la empresa Imperva en el año 2015, su informe denominado Web Application Attack Report con sus siglas en inglés *(WAAR)*, analizó 297 954 ataques, además de 22 850 023 alertas en 198 aplicaciones web, en un lapso de 6 meses, se pudo notar el incremento de ataques web. El tipo de ataque más relevante fue inyección SQL [5].

Akamai Technologies también realizó un informe de seguridad acerca del estado de internet en los tres primeros meses del año 2016, y los comparó con los cuatro primeros meses del año 2015, obteniendo como resultado un incremento del total de los ataques realizados a aplicaciones web en un 25,52%, además también se presentó un incremento del 87,32% en los intentos de acceso del tipo inyección SQL. Los ataques sobre el protocolo HTTP representaron un 89,75% [6].

En el estudio que realizó Toshiki Shibahara y Yuta Takata (2019) indican las amenazas a las que están expuestas las empresas que manejan la web sean estas públicas o privadas, y la forma de operar de los atacantes redirigiendo a los clientes a sitios maliciosos para poder hurtar información [7].

1.2 ARQUITECTURA DE UN SITIO WEB

La arquitectura web consiste en crear aplicaciones que de forma posterior será presentada a través de la web, haciendo uso del protocolo HTTP para que se cree relaciones entre el cibernauta y otras aplicaciones web[8].

La arquitectura web tiene requisitos propios, que serán analizados a continuación

Diseño de interfaz de usuario. - Es el diseño web, la estructura de sus contenidos y su aspecto visual, en esta parte de la arquitectura los protagonistas son el diseño gráfico, la facilidad de uso, la experiencia del cibernauta, mapas del sitio o mapas web, también los distintos estándares web como HTML, CSS, DOM, AJAX Y JAVASCRIPT.

Diseño e implementación de la lógica de la aplicación. - El sitio web ofrecerá funcionalidades tanto en el diseño como en la ejecución de los algoritmos, también en la manera con la que la información almacenada será manipulada, es decir el planeamiento y el diseño que llevará consigo al funcionamiento de uno o varios lenguajes de programación.

Diseño de la arquitectura de la información. - Establecer la información con la que tendrá que trabajar la aplicación, mediante diseño del modelo conceptual, de sus entidades y relaciones, para determinar el modelo de datos, adquiriendo un modelo conceptual que se adapte, y así llevar a cabo la implementación del modelo de datos sobre una base de datos, realizando el traslado de la información necesaria y obtener el funcionamiento correcto [9], ver Ilustración 1.

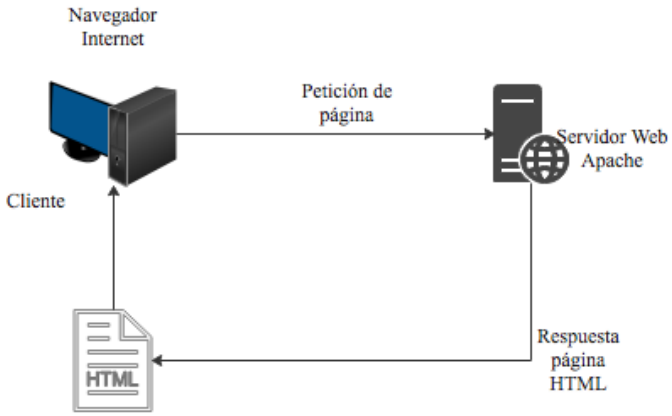

Ilustración 1. Arquitectura de un sitio web

1.3 SEGURIDAD

La seguridad es un proceso, por ende, es un conjunto de procedimientos y herramientas con la finalidad de proteger los datos y recursos informáticos frente a las amenazas que se presenten.

Existe el tipo de Seguridad de la información y seguridad informática a pesar de que tengan similitud son conceptos diferentes, la seguridad de la información hace referencia a la falta de normas, políticas, ausencia de control de cambios, procedimientos, educación de usuarios y conocimiento de la misión de la organización, mientras que, la seguridad informática tiene se enfoca en virus, spam, contraseñas y ataques Ddos.

SEGURIDAD DE LA INFORMACIÓN

Son los datos lo cuales una organización mantiene, si esta información se pierde, deteriora o es hurtada puede hacer que la empresa baje sus niveles de competencia y le será difícil recuperarse, por este motivo se requiere que la seguridad de la información esté ligada a la seguridad informática para poder implantar políticas de seguridad y hacer seguimientos de estas[10]. La norma ISO 27001 no solo reduce riesgos y amenazas, también mejora la planificación y gestión de la seguridad de una organización y proporciona prestigio [11].

La seguridad de la información maneja algunos aspectos, pero entre los principales se puede obtener la confidencialidad es donde solo puede tener acceso personal autorizado durante el proceso de almacenamiento, procesamiento o transmisión. Además, la integridad también forma parte de los aspectos principales y en este paso los datos solo pueden ser modificado y eliminados por quien esté apropiadamente autorizado, en esto se incluye la autenticidad, no repudiación y contabilidad. Por otra parte, la disponibilidad, los datos deben estar disponibles para poder ser accedido por personal autorizado, cuando sea requerido [12].

SEGURIDAD INFORMÁTICA

Asegura los recursos del sistema de información por esa razón están ligados.

Tiene como objetivo poseer un nivel de seguridad aceptable, para poder mitigar los ataques de los potenciales intrusos logrando que fracasen en los intentos de ataque [13].

1.3.1 VULNERABILIDADES

Los atacantes hoy en día pueden hallar debilidades de las aplicaciones en la red. Existe una vulnerabilidad llamada día cero que al explotar, los hackers pueden llegar a tener acceso a la red de destino y hurtar información íntima [14].

En la seguridad informática la vulnerabilidad es una debilidad y un error involuntario en un sistema o en el código del software. Para que un intruso pueda acceder a un sistema que tenga debilidades necesita de técnicas y herramientas para conectarse [15].

1.3.2 AMENAZAS

AMENAZAS INTERNAS

Las amenazas internas causan más daños que las externas, porque son manipuladas por los usuarios internos que tiene acceso a la infraestructura de los sistemas.

Las razones por lo que existen las amenazas internas es por que alguien del personal interno puede de forma incorrecta manipular datos confidenciales, al conectar dispositivos infectados facilitar los ataques externos o de forma accidental invitar malware (correos electrónicos, páginas web maliciosos) [16].

AMENAZAS EXTERNAS

Las amenazas externas son las que se realizan por atacantes que no pertenecen a la empresa, los que están al asecho por medio de la red buscando el momento preciso para atacar por lo general este tipo de atacantes manejan estrategias para poder realizar los ataques tales como la noche, fines de semana o días festivos.

1.3.3 ATAQUES

ATAQUES DE INYECCIÓN SQL

Los ataques de inyección en las aplicaciones web suceden cuando se ejecuta sentencias de SQL dinámicas, es considerado uno de los más peligrosos ataques web, por el motivo de que ataca ingresando a la información de un formulario web para tener acceso a una cuenta o a su vez modificar los datos [3].

ATAQUES DOS

El ataque DoS (Denegación de Servicio) consiste en generar una cantidad masiva de peticiones al servicio desde un ordenador, comenzando a rechazar peticiones después de consumir los recursos que ofrece el servicio hasta que no tiene capacidad de respuesta [17].

ATAQUES DDOS

El ataque DDoS (Denegación de servicio distribuido) malicioso empieza con la interrupción de los servicios que ofrece un sistema a sus usuarios genuinos, este ataque se llama DDOS, es eficaz que causa perdidas para grandes organizaciones, incluyendo las gubernamentales [18].

Este tipo de ataques requiere métodos precisos y adaptables, tiene que ser detectada a tiempo porque imposibilita que el sistema provea servicio a sus usuarios [19].

ATAQUES DE FUERZA BRUTA

Estos tipos de ataques rompen todas las combinaciones posibles, nombres de usuarios y contraseñas en una página web, además, los ataques por fuerza bruta buscan contraseñas vulnerables que puedan ser descifrables y permitan el acceso al servidor [20].

CROSS SITE SCRIPTING

Cross-Site Scripting (XSS) es usado por los atacantes para inyectar scripts maliciosos en sitios web. Estos atacantes utilizan XSS para que el script malicioso sea enviado a cualquier usuario desprevenido que esté haciendo uso del navegador y no tiene forma de saber que este script es malicioso y lo ejecutará [21].

1.3.4 HACKING ÉTICO

Los hackers o ciber delincuentes puede ser cualquier persona que utiliza sus conocimientos en hardware y software para romper y eludir la seguridad, dependiendo de sus intenciones se lo clasifica como “Black Hat” y “White Hat”

- Black Hat:

Los hackers de sombrero negro generalmente tienen un amplio conocimiento sobre cómo ingresar a las redes informáticas y eludir los protocolos de seguridad también son responsables de malware, que es un método utilizado para obtener acceso a los sistemas.
La motivación de los black hat es obtener ganancias personales o financieras, pero también pueden verse involucrados en espionaje cibernético, se caracterizan por ingresar al sistema sin el permiso del propietario.

- White Hat

Los hackers de sombrero blanco son conocidos como “hackers éticos”, son especialistas en seguridad los cuales usan sus conocimientos para encontrar problemas de seguridad a través de la piratería, emplean el mismo método que los black hat con la diferencia que lo hacen con el permiso del propietario del sistema, haciendo el proceso legal.

Una característica de los White hat es que las distintas pruebas de vulnerabilidad realizadas son notificadas a las empresas para su pronta corrección y buen funcionamiento [15].

En la puesta en marcha del ethical hacking y la protección de la red, sería complicado lograr protección exitosa si no se logra comprender las vulnerabilidades de los sistemas informáticos [22].

1.3.5 HARDENING EN SERVIDORES

Hardening es el proceso de medidas de seguridad y endurecimiento que se realiza al configurar los servidores, este proceso se realiza para que no quede las configuraciones por defecto, para esto se requiere de el cierre de los puertos que no se van a usar, la pronta eliminación de usuarios que no sean los que se requieren, y se configura para lograr credenciales más seguras [23].

Las medidas que se toman en el proceso de hardening con ayuda del administrador del equipo se busca reforzar la seguridad. El propósito dificultar las acciones del atacante para evitar que este se concrete.

Entre los objetivos de hardening está: Disminuir las vulnerabilidades del sistema y el impacto de un suceso de seguridad, optimizar la administración del sistema al identificar de forma más óptima la causa de una eventualidad al poder retirar las causas que ya se tomaron acciones con el proceso de hardening [24].

1.3.6 HERRAMIENTAS DE ESCANER

Según Y. Wang las mejores herramientas de escaneo son las que se detallan a continuación.

Nmap: Proporciona una flexibilidad, simplicidad y portabilidad en la obtención de paquetes de filtros y cortafuegos. Realiza escaneo de redes grandes y pequeñas. Su portabilidad se debe a que es soportado por algunos de los más populares sistemas operativos(LINUX, WINDOWS, SOLARIS, MAC OS) [9].

Wireshark: Intercepta el tráfico y lo convierte en un formato legible para las personas, permite identificar el tráfico que cruza por la red en tiempo real.

Comando Nikto: Escanea los servidores web en busca de archivos peligrosos, malas configuraciones y vulnerabilidades en el servidor.

Sslabs: Escanea dominios y hosting para la verificación de configuración mostrando como resultado una calificación que permitirá verificar la efectiva o no configuración del servidor.

1.4 SISTEMAS OPERATIVOS

Existen diferentes tipos de S.O, para ordenadores iOS, Linux y Microsoft de los cuales el único sistema operativo libre es Linux.

Linux al ser un sistema operativo de código abierto permite que sea adaptado a las necesidades y requerimientos de quien adquiera este S.O, a diferencia de Mac OS X y Microsoft que son de paga y solo tiene acceso al código su propio personal [25].

En la línea Linux existen algunos sistemas operativos como Mandriva, Suse, Ubuntu, Centos, Debian, Fedora, entre otros.

Tabla 1. Años de soporte de S.O Linux

SISTEMAS OPERATIVOS LINUX	AÑOS DE SOPORTE
RED HAT	10
CENTOS	10
UBUNTU	5
FEDORA	1
DEBIAN	3

En la ***Tabla 1***. Se detalla los años de soporte que tiene cada sistema operativo basado en Linux como parte de la investigación para bases de la elección del S.O con que se va a trabajar.

1.5 SERVIDOR

Es un ordenador o programa informático que posee una función dentro de una red de forma específica, los servidores son utilizados para brindar servicios a los equipos que se encuentran conectados entre sí [26].

Para hacer una selección correcta de un servidor se requiere conocer las necesidades reales y realizar una proyección hacia el futuro de una organización

porque de esto va a depender el correcto funcionamiento, la seguridad y los procesos diario de automatización.

La función principal de los servidores es orientar y enfocar la información, centralizar las aplicaciones (correo, archivos, web, programas) y tener estandarizadas las operaciones de una organización.

APACHE

Apache es un servidor web open source, y según estadísticas es uno de los más utilizados en el mundo, es flexible y puede ser empleado en distintos sistemas operativos (Linux, Windows, MacOs), la instalación depende del sistema operativo y de los requerimientos que se tengan para este servidor dependiendo de las necesidades del empleador de este.

DOCKER

Esta tecnología muestra las aplicaciones dentro de contenedores de software, es de código abierto y permite empaquetar una aplicación y sus dependencias, su flexibilidad y portabilidad permite que sea ejecutable en cualquier tipo de servidor. Una imagen de contenedor de Docker es un paquete de software ligero, el cual contiene la información necesaria para ejecutar una aplicación: código, tiempo de ejecución, herramientas y bibliotecas del sistema.

Las imágenes de contenedores se convierten en contenedores en tiempo de ejecución, el software en contenedores se ejecutará siempre de la misma manera independientemente de la infraestructura.

Por medio de contenedores, los recursos pueden ser aislados, y puede otorgarse a cada proceso la capacidad tener una visión privada del sistema operativo, pueden existir contenedores múltiples que comparten el mismo núcleo, pero cada contenedor puede ser restringido a usar cierta cantidad de recursos, como por ejemplo memoria [27].

1.5.1 FIREWALL DE APLICACIONES WEB

Para identificar y restringir los ataques de scripts entre sitios un firewall de aplicaciones web aplica un conjunto de reglas. Los firewalls de aplicaciones web permite personalizar las reglas identificando y bloqueando contenido malicioso.

En los últimos años la tecnología ha tenido un notorio crecimiento en el desarrollo y ejecución de aplicaciones web como asistente de servicios a través del internet.

Y con este notorio crecimiento también se desatan los problemas de seguridad, siendo objetivos de los ataques cibernéticos, lo que causa perturbación de los servicios y pérdidas de dinero [28].

Para los sistemas de software online los WAF son un elemento de protección, para evitar que los hackers ingresen con facilidad, los software de aplicaciones web deben ser restaurados y analizados de forma regular [29].

Tabla 2. Beneficios, Ventajas y desventajas de aplicar firewall en aplicaciones web

Beneficios	Ventajas	Desventajas
• Brinda protección desde su implementación. • No se requiere la modificación del código de las aplicaciones web.	• Detecta y bloquea ataques antes de que alcancen a las aplicaciones web • No importa el lenguaje y plataforma de desarrollo de la aplicación web. • Protege cualquier servidor web. • Variedad de soluciones WAF open source y de paga.	• Requiere de un periodo de pruebas y adecuación. • Consume más recursos (Procesador, Ram) • Si las aplicaciones web cambian, puede que se requiera adecuar el WAF a los cambios.

En la ***Tabla 2***. Se detalla los beneficios, ventajas y desventajas del uso de WAF, que se debe tener en cuenta previo la implementación

1.5.2 MODSECURITY

Modsecurity es un módulo de seguridad que se configura en el servidor web apache, para la función correcta de este firewall debe estar configurado con normas apropiadas, al tener las reglas óptimas hará que el cortafuego identifique los ataques correctamente, permitiendo examinar la comunicación HTTP, donde puede encontrar ataques desconocidos [30].

Este módulo en el nivel de aplicación forma una capa de seguridad y en la comunicación HTTP actúa como firewall. Al mismo tiempo analiza las peticiones HTTP, puede ser en la propia URL o a su vez mediante el método POST que se encarga de buscar los patrones que han sido definidos por el usuario, con el objetivo de evitar ataques de inyección SQL [31].

El módulo Modsecurity permite la colaboración de otros módulos de Apache con el objetivo de fortalecer y reducir los ataques.

NIVEL DE PARANOIA MODSECURITY

El conjunto de reglas principales de Modsecurity CRS de OWASP son reglas de firewall, que se cargan en firewalls de aplicaciones web compatibles. CRS contiene algunos archivos .conf que cuentan con firmas genéricas para cada categoría de ataque, como inyección SQL.

Las configuraciones de nivel de paranoia PL permite elegir el nivel que se desea de verificación de reglas, dicha configuración se la realiza en crs-setup.conf que es un archivo de VirtualHost.

En cada aumento de PL, el CRS habilita reglas adicionales, brindando una mayor seguridad. No obstante, los niveles más elevados de paranoia también aumentan la posibilidad de bloquear tráfico legítimo debido a falsas alarmas o falsos positivos “PF”. Si se usan PL más altos, se deberá añadir reglas de exclusión para ciertas aplicaciones. [32]

Primer nivel de paranoia (PL1) en este nivel la mayoría de las reglas principales están habilitadas. Es para principiantes y para aplicaciones con requisitos de configuración estándar.

Segundo nivel de paranoia (PL2) es un tipo de nivel para usuarios moderados a experimentados, y para las instalaciones con requisitos de seguridad elevados, incluye muchas reglas adicionales como son las protecciones para ataques de inyección, estas reglas agregan protección adicional que en PL1 son fácil de evadir.

Tercer nivel de paranoia (PL3) permite más reglas y listas de palabras claves para los ataques menos comunes, ajusta los límites de los caracteres especiales utilizados, lo que genera un mejor control y una alta cobertura de los ataques desconocidos e intento de omisión de WAF, PL3 está dirigido para usuarios con experiencias en el manejo de filtros de paquetes PF y en instalaciones con altos requisitos de seguridad.

Cuarto nivel de paranoia (PL4) es recomendable para usuarios experimentados que protegen instalaciones con requisitos de seguridad muy altos porque hace restricción de caracteres especiales de forma más estricta, la ejecución de PL4 produce una gran cantidad de PF que deben ser tratado antes que el sitio sea productivo.

1.5.3 MOD_EVASIVE

Es un módulo de Apache diseñado para ser una herramienta de detección y gestión de la red, proporciona una acción de protección en caso de un ataque de denegación a su vez puede ser configurado para tener comunicación con ipchains, firewall, routers.

1.6 CERTIFICADOS DE SEGURIDAD

Son un extra en seguridad para la información de las personas que visitan páginas web, los certificados encapsulan la información para evitar que sujetos mal intencionados tengan acceso [33].

Se puede saber si una página web cuenta con certificados si al añadir la dirección en la barra de direcciones se refleja el protocolo HTTPS, o a su vez se refleja un candado, si está bien configurado se reflejan ambos, cuando no está bien configurado se refleja un signo de admiración y la palabra no seguro [34].

1.7 BASES LEGALES

En la presente investigación según los fundamentos en los que se establece hace el uso de software libre, en la Constitución de la República del Ecuador se encuentra representada por el Decreto 1014.

Según el Art. 1 del decreto 1014 establece como política la utilización de software libre en su sistemas y equipamientos en la administración pública, también indica que debe ser evaluador de forma regular los sistemas informáticos, en el mismo decreto el Art. 4 indica el permiso obtenido para software propietario únicamente cuando no exista una solución de software libre que cumpla las necesidades requerida [35].

En el Código Orgánico de la Economía Social de los conocimientos, creatividad e innovación del Ecuador, en el Art. 142 se indica la libertad de usar software libre para cualquier propósito, la libertad de analizar y estudiar el software libre para adaptarlo a las necesidades requeridas, y la libertad de distribuir copias de las adaptaciones a terceros [36].

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1 TIPO DE INVESTIGACIÓN

Esta investigación tuvo tres enfoques, cualitativo, cuantitativo y experimental. Cualitativo porque la información que se utilizó es de investigaciones previas de diferentes investigadores alrededor del mundo, cuantitativo debido a que se analizó los certificados de seguridad de algunas páginas web y por otro lado experimental porque de acuerdo con la información recopilada se puso en práctica la configuración del firewall para reducir las amenazas. Para el cumplimiento de estos propósitos se llevaron a cabo 2 etapas.

La primera etapa se centró en el análisis tomando como referencia información de investigaciones realizadas con anterioridad para lograr obtener los conocimientos necesarios y definir el uso de las tecnologías. Definiendo el uso de GOOGLE CLOUD SERVICES para la creación del entorno virtual. Realizando pruebas de seguridad a sitios web y concluyendo que estas carecían de certificados de seguridad y calificación menor de A+.

En la segunda etapa se logró poner en práctica dos escenarios que se desarrollaron creando una máquina virtual que cuenta con Centos. Dentro de un contenedor en donde ambos son configurados con dockercompose.yml haciendo uso del servidor web Apache.
En el primer escenario se encuentra la configuración básica sin seguridad alguna. En el segundo escenario se encuentra los módulos de seguridad que fueron propuestos como parte de los objetivos de este trabajo de investigación, como son fail2ban, mod evasive y el firewall modsecurity. Adicionalmente, se realizó la configuración del servidor para la obtención de la calificación más alta la cual certifica la buena configuración de este, y finalmente en ambos escenarios se realizaron ataques de denegación de servicio.

2.2 MÉTODOS

Para el desarrollo de esta investigación se ejecutó el servidor web Apache debido a que es uno de los servidores opensource con carcterísticas relevantes y más usado según la compañía Netcraft, es una empresa dedicada a las mediciones del uso de los diferentes servidores web. Apache es multiplataforma y permite emplear diversos lenguajes e implementación de conexiones seguras.

Para esto se levantó información cuantitativa para obtener datos reales de los diferentes tipos de certificados con los que cuentan los sitios web, y experimental para configurar el firewall.

Método Inductivo: Permitirá identificar las amenazas por medio de la información obtenida de las herramientas para reducir las vulnerabilidades.

Método Deductivo: Se podrá definir los hechos concretos de la puesta en práctica de la investigación a realizar.

2.3 INSTRUMENTOS

La investigación netamente es experimental por este motivo con la aplicación de los métodos de investigación antes mencionados se configuro un servidor con el sistema operativo CentOS, se realizó dos tipos de prueba el primero sin ningún tipo de seguridad ni certificados y el segundo con certificados protocolos de seguridad válidos y actualizados, se realizó los ataques respectivos y se obtuvieron los siguientes resultados.

CAPÍTULO III: RESULTADOS

Para el proceso experimental se realizó el levantamiento de una página web con el CMS Wordpress en un entorno que se encuentra con el servidor web apache. En este punto es necesario verificar los puertos que se encuentran abiertos y cerrados del servidor para poder ser habilitados o deshabilitados según se requiera, para este cometido se utilizó el comando Nmap, ver Ilustración 2.

Ilustración 2. Comando Nmap

En el siguiente apartado se encuentra la información que se visualiza en Ilustración 2 pero en una tabla para su mejor entendimiento, ver ***Tabla 3***.

Tabla 3. Detalle de puertos del servidor

Puerto	Protocolo	Status	Servicios	Versión
22	TCP	Abierto	SSH	OPENSSH 7.4
80	TCP	Abierto	HTTP	APACHE HTTPD2.4.38
443	TCP	Abierto	HTTPS	

En la **Tabla 3** se detalla los puertos, protocolos, servicios y versión que se encuentran funcionando en el servidor.

En la siguiente ilustración se pudo verificar que el método TRACE no estaba activo, en algunas investigaciones sugieren desactivar este método en el caso de que se encuentre activo por el hecho que desata riesgos, permite a un atacante robar información y credenciales de un sitio, ver Ilustración 3.

```
+ Target IP:          35.198.59.147
+ Target Hostname:    35.198.59.147
+ Target Port:        80
---------------------------------------------------------------------------
+ Server: Apache/2.4.38
+Retrieved x-powered-by header: PHP/7.3.17
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ wp-links-opml.php: This Wordpress script reveals the installed version.
+ OSVDB-3233: /license.txt: License file found may identify site software
+ /wp-app.log: Wordpress wp-app.log may leak application/system details.
+ /wordpress/: A Wordpress installation was found
+ Cookie wordpress_test_cookie created without the http only flag
+ 23695 requests: 0 error(s) and 3 item(s) reported on remote host
```

Ilustración 3. Usando comando nikto para escaneo de puertos.

Antes de realizar los ataques al servidor se realizó un escáner del hosting con la herramienta SSL Labs que mostró un resultado de evaluación fallida y que no se puede establecer conexión con el servidor, ver Ilustración 4.

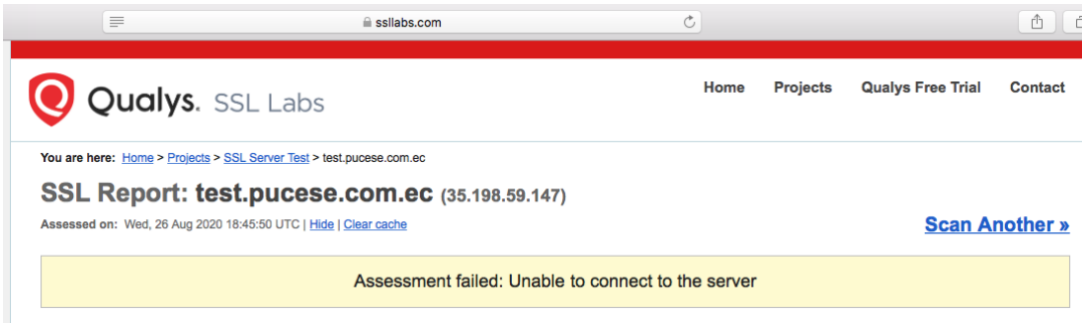

Ilustración 4. Scanner de página web sin protocolos de seguridad

Escenario 1 ataques a la página web sin protocolos de seguridad

Ataque DoS

La denegación de servicio fue llevada a cabo con el programa DoSer el cual permitió enviar cantidades de peticiones también conocido como paquetes, hasta que logró dejar sin servicio la web.

Envío de paquetes que dejará sin servicio el sitio web, ver Ilustración 5.

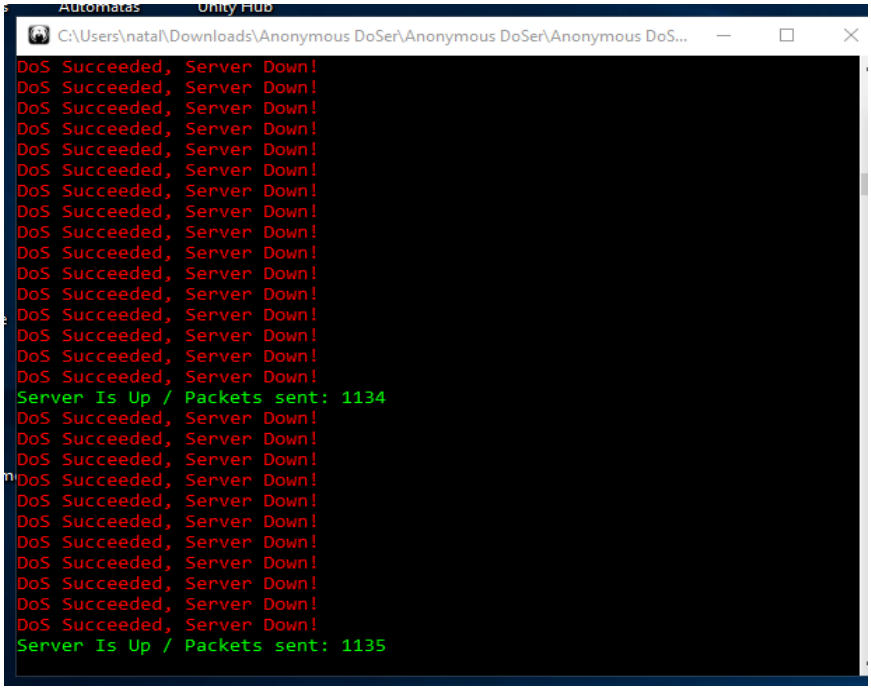

Ilustración 5. Dejar sin servicio página web

Ataque DDoS

Se realizó el ataque DDoS con la herramienta hping3 disponible en kali linux, ver **Error! Reference source not found.**.

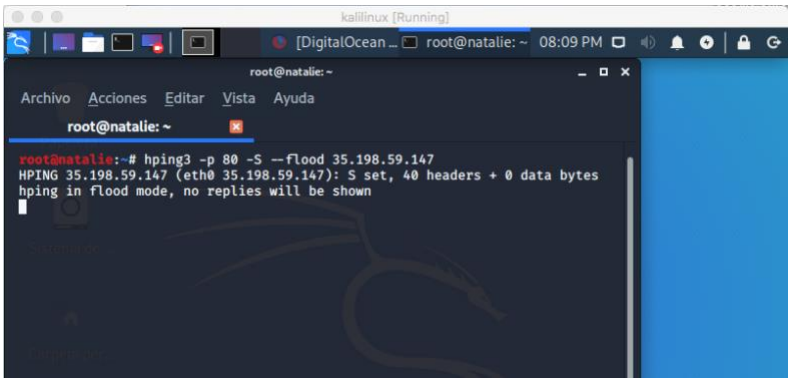

Ilustración 6. Ataque DDos con hping3

Al finalizar los ataques se logró visualizar que ambos lograron dejar sin servicio al servidor.

Escenario 2 con protocolos de seguridad y Modsecurity

Al tener configurado el certificado digital y Modsecurity instalado no permitirá que los ataques afecten al servidor, en este segundo escenario se realizó los mismos ataques que en el escenario 1 para dar valor crítico entre estos dos ambientes.

En este escenario el hecho de tener certificado digital ya califica al sitio como seguro.

En este segundo escenario se realizó la instalación de los módulos de seguridad, fail2ban, mod_evasive y modsecurity

En fail2ban se instaló y se configuró el archivo jail.local, en este archivo se modificó los siguientes parámetros.

"bantime" es el número de segundos que un anfitrión está prohibido.
bantime

Un huésped está prohibido si ha generado "maxretry" durante el último "findtime" segundos.
findtime

"maxretry" es el número de fallos antes de que un anfitrión sea prohibido.
maxretry
Se reinició el sistema y se verificó el estado del fai2ban, ver Ilustración 7.

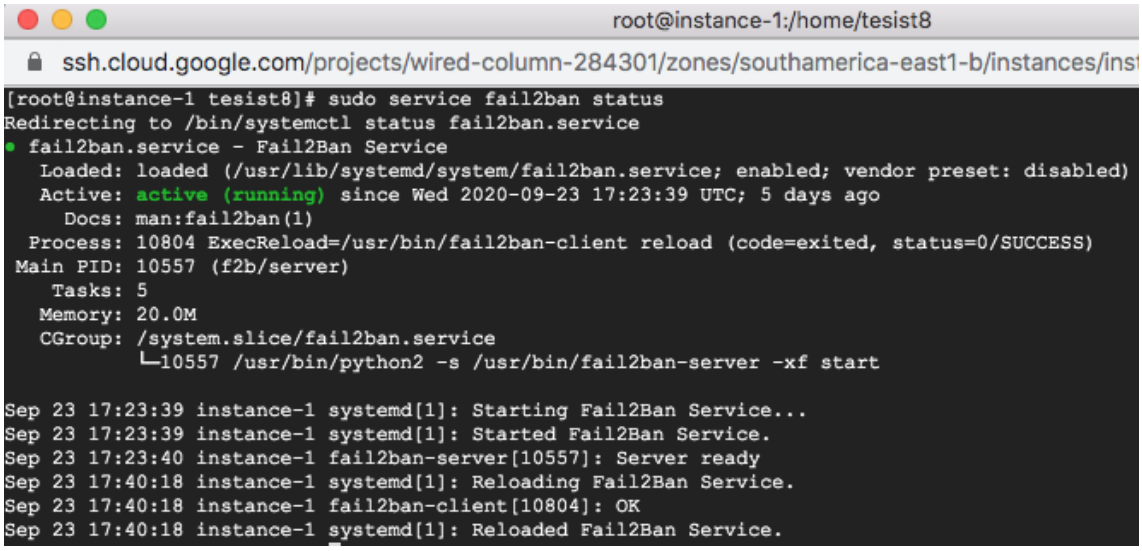

Ilustración 7. Fail2ban activado

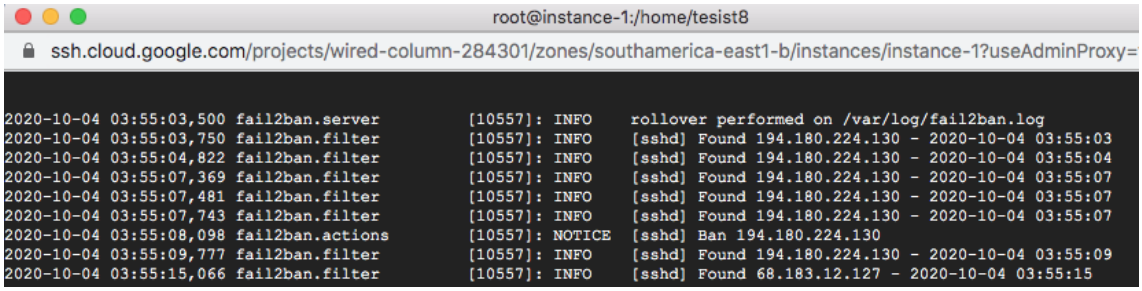

Ilustración 8. Ataques detectados por fail2ban

El siguiente modulo en instalar fue Mod_evasive se configuró el archivo que se encuentra alojado en nano etc/apache2/mods-enable/evasive.conf, ver Ilustración 9, se verificó que esté habilitado ver Ilustración 10.

Ilustración 9. Configuración de mod_evasive

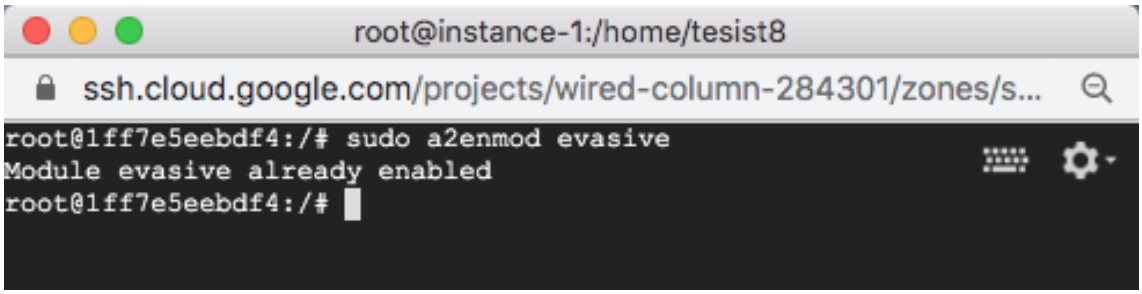

Ilustración 10. Mod_evasive activado

En última instancia se instaló y configuró Modsecurity, como se puede visualizar en las siguientes ilustraciones.

Se realizó la instalación de modsecurity con el siguiente comando, apt install libapache2-mods-security2 modsecurity-crs, se agregó modsecurity crs para que con este comando se agreguen las reglas para no ser instalados por separado, ver Ilustración 11.

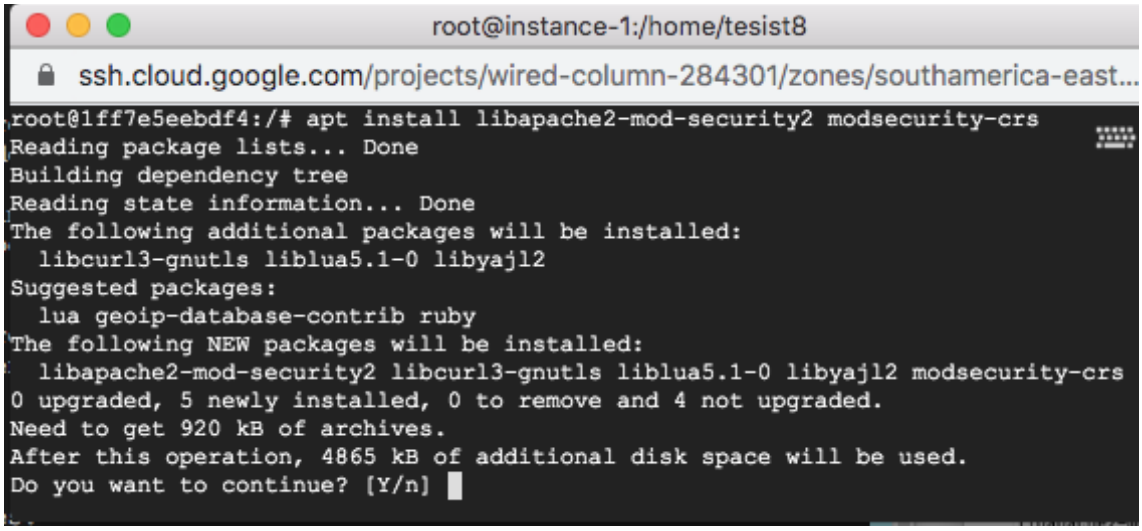

Ilustración 11. Instalación de modsecurity y su conjunto de reglas

Luego se procedió a la activación de la sección de reglas para poder usarlas, se ingresó al directorio usando el siguiente comando cd /etc/modsecurity/, nano modsecurity.conf y donde se encontraba SecRuleEngine DetectionOnly se le cambió por SecRuleEngine On, ver Ilustración 12.

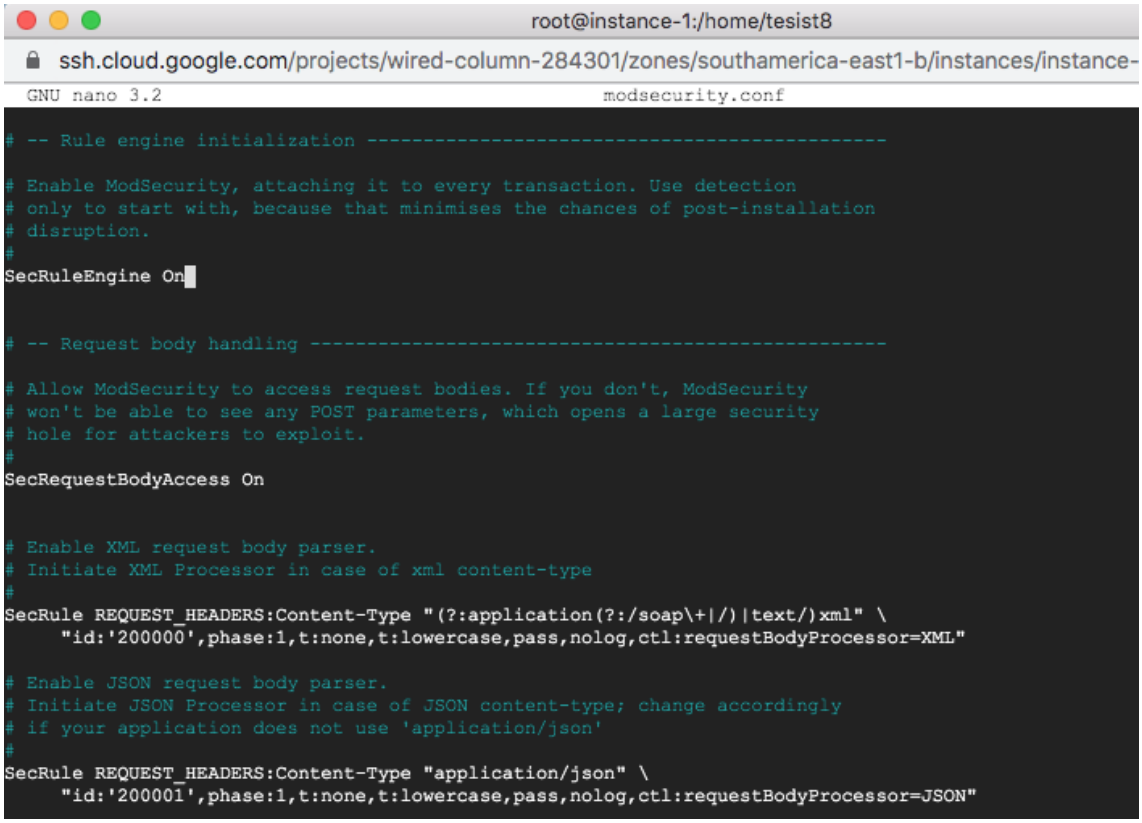

Ilustración 12. Activación de reglas Modsecurity

Se verificó los niveles de paranoia ingresando el siguiente comando cd /etc/modsecurity, nano crs-setup.conf en el cual aparte de los niveles de paranoia también muestra información sobre la versión de modsecurity que se tiene instalada.

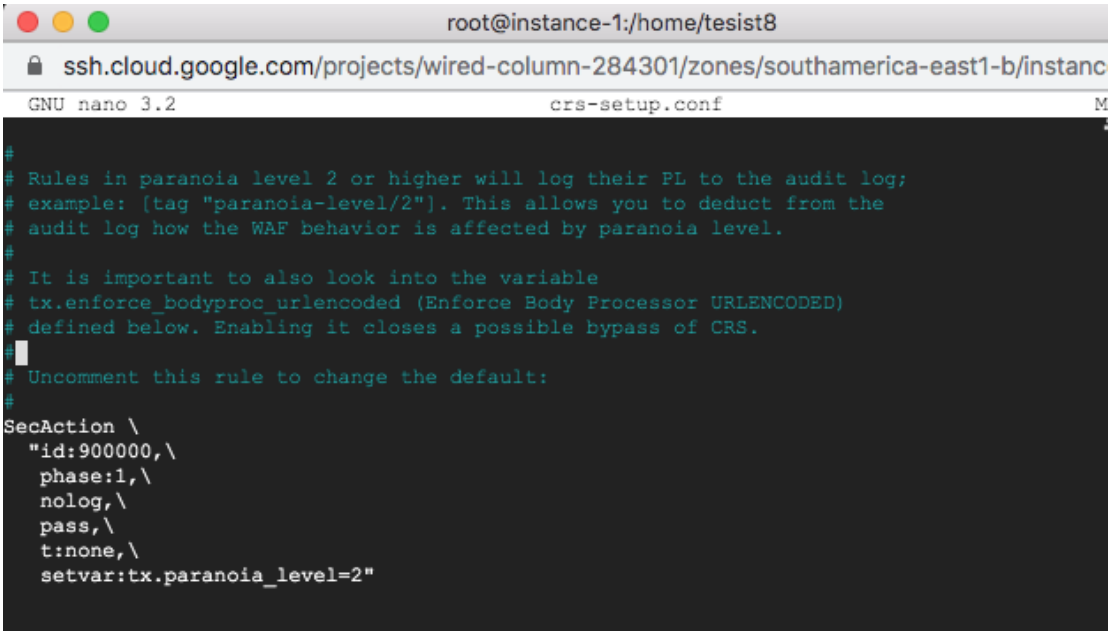

Ilustración 13. Activar nivel de paranoia

Se ejecuta una regla de prueba en /usr/share/modsecrity-crs/rules/test.conf la cual al recibir el ataque mostrará la página 403 Forbidden, ver Ilustración 14.

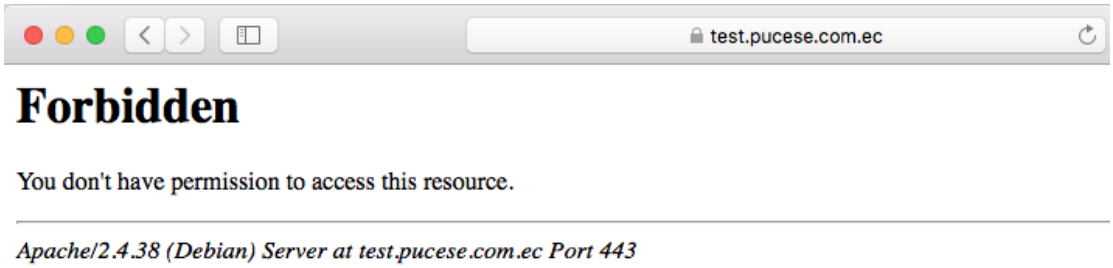

Ilustración 14. Prueba de regla establecida

Ataque DoS

Al igual que en el escenario 1 se procedió a realizar los ataques, haciendo uso de las mismas herramientas, pero con los módulos de seguridad empleados. Este proceso es vital porque permite verificar la efectividad del firewall y si un servidor puede manejar la cantidad de paquetes que son enviados para dejar sin servicio un servidor. Ataque realizado con la herramienta Anonymous DoSer

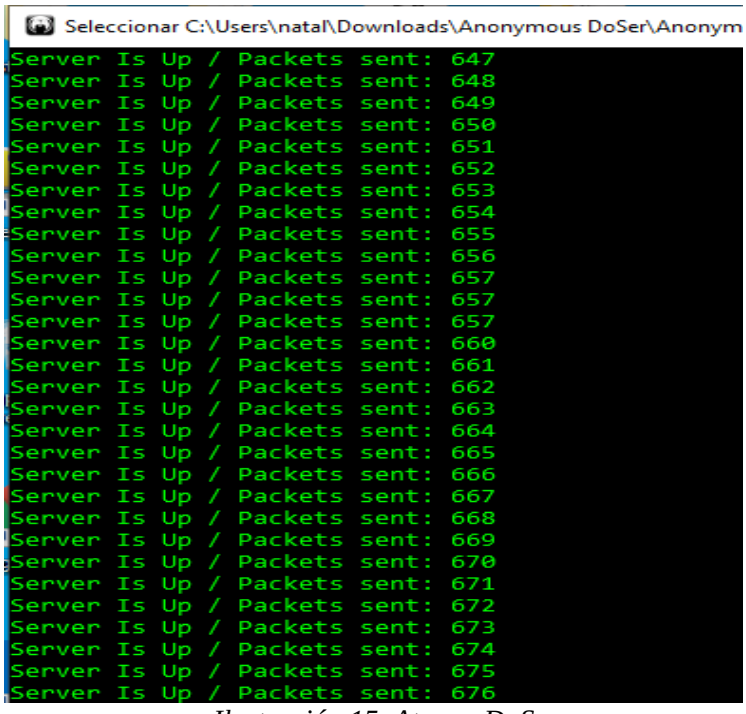

Ilustración 15. Ataque DoS

Ataque DDoS

Con la herramienta hping3 se llevó acabo el ataque DDos.

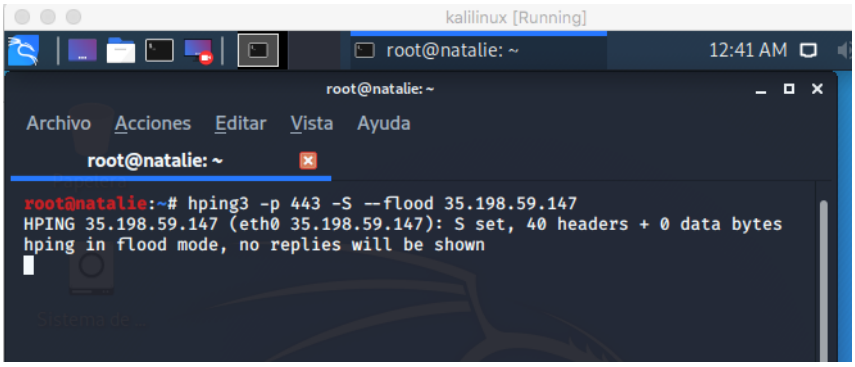

Ilustración 16. Realizando Ataque DDoS

Al finalizar los ataques se obtuvo que las configuraciones realizadas están correctas al no tener afectaciones.

En el último punto se logró configurar SSL para obtener la calificación A+ lo cual es significativo ya que al tener un A+ indica la correcta configuración del servidor, ver Ilustración 17, esta configuración fue realizada en nano etc/letsencrypt/options-ssl-apache.conf y nano etc/apache2/mods-available/ssl.conf modificando SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 en ambos archivos.

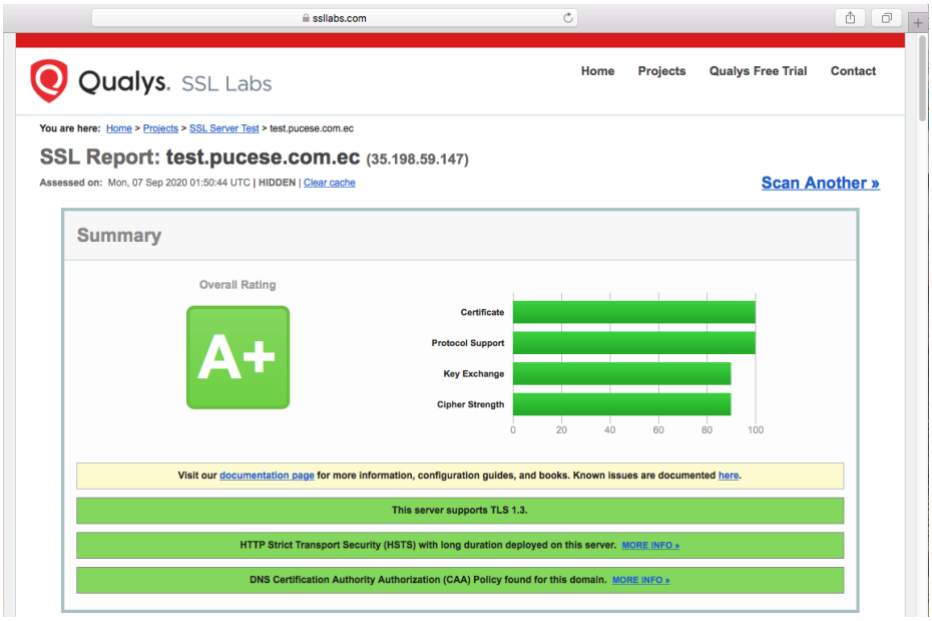

Ilustración 17. Calificación A+ en sitio web

CAPÍTULO IV: DISCUSIÓN

El objetivo de la investigación presentada es reducir las vulnerabilidades de un servidor Web mediante el fortalecimiento de la seguridad, haciendo uso del Web Application Firewall conocido por sus siglas en inglés (WAF) de aplicaciones web Modsecurity.

Por la mala configuración del servidor web o por no saber el estado del mismo, ni de las herramientas que operan para la reducción de inseguridad, Toshiki Shibahara [7] indica en su estudio que las empresas privadas y públicas que hacen uso de la web, están expuestas a amenazas. Existen herramientas que ayudan a verificar el estado del servidor que fueron usadas en este trabajo como lo son el comando nikto y nmap los cuales ayudaron mostrando los puertos abiertos y cerrados del servidor, a su vez, la herramienta online ssl labs permitió la calificación máxima de seguridad al mostrar los suites de cifrado y certificados que carecía.

Hurtado en su investigación [37] nombra a los certificados digitales como herramientas tecnológicas, los cuales son emitidos por Let’s Encrypt, indicando que la configuración e implementación de certificados digitales SSL brindan seguridad. Hurtado pudo comprobar que el solo uso de certificados digitales contrarresta ataques como pishing, sin embargo no contrarrestó ataques más potentes como DoS y DDosS por esto, fue necesario implementar módulos de seguridad como son fail2ban y modevasive, los cuales al estar debidamente configurados contrarestaron los ataques.

CAPÍTULO V: CONCLUSIONES

- Con los resultados obtenidos en esta investigación, se demuestra que se cumplieron los objetivos planteados, objetivos que se lograron alcanzar por medio de la recopilación de información veraz, logrando fortalecer la seguridad del servidor web.

- La configuración del firewall de aplicaciones web Modsecurity fue instalado en el servidor y se le implementó niveles de paranoia (PL), los mismos que permitieron registrar y bloquear solicitudes maliciosas que pudieran afectar los datos del cibernauta.

- Por medio de los resultados se visualizó que el uso de la herramienta fail2ban logró mitigar la denegación de servicio DoS, mostrando un informe de los atacantes y al mismo tiempo bloqueando su intento de acceso al servidor.

- Finalmente, la implementación de mod_evasive permitió frenar los ataques DDoS al recibir peticiones de acceso, anulando las peticiones recibidas desde una o varias IP.

CAPITULO VI: RECOMENDACIONES

- Hacer uso de contenedores, puesto que, permitió generar dos entornos en la parte experimental de este trabajo. Docker permite tener dependencias juntas.

- Actualizar los certificados SSL debido a que los sitios web sin certificados digitales actualizados, no poseerán el protocolo de seguridad (https), por lo tanto, son más propensos a recibir ataques.

- Obtener la calificación A+ porque indica la correcta configuración del servidor.

Bibliografía

[1] B. Li, G. Yuan, L. Shen, R. Zhang, and Y. Yao, "Incorporating URL embedding into ensemble clustering to detect web anomalies," *Futur. Gener. Comput. Syst.*, vol. 96, pp. 176–184, 2019.

[2] J. David and C. Thomas, "Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic," *Comput. Secur.*, vol. 82, pp. 284–295, 2019.

[3] D. Das, U. Sharma, and D. K. Bhattacharyya, "Defeating SQL injection attack in authentication security: an experimental study," *Int. J. Inf. Secur.*, vol. 18, no. 1, 2019.

[4] T. PEREZ, "Website Application Firewalls (WAF) - Un Enfoque Práctico para la Seguridad de Sitios Web," *February*, 2017. [Online]. Available: https://blog.sucuri.net/espanol/2017/02/website-application-firewalls-waf-un-enfoque-practico-para-la-seguridad-de-sitios-web.html. [Accessed: 18-Jul-2019].

[5] Imperva, "2015 Web Application Attack Report (WAAR)," p. 37, 2015.

[6] Akamai Technologies, "Akamai publica el informe de conectividad sobre el estado de Internet del primer trimestre de 2016 | Akamai ES." [Online]. Available: https://www.akamai.com/es/es/about/news/press/2016-press/akamai-first-quarter-2016-state-of-the-internet-connectivity-report.jsp. [Accessed: 18-Jul-2019].

[7] S. Similarities, T. Shibahara, Y. Takata, M. Akiyama, and T. Yagi, "Evasive Malicious Website Detection by Leveraging Redirection," no. xx, pp. 1–14, 2019.

[8] L. E. Paz Enrique and L. L. Cuellar Santos Suárez, "Diseño de la arquitectura de información del sitio web de la Facultad de Ingeniería Industrial y Turismo de la Universidad Central 'Marta Abreu' de Las Villas," *Cuad. Doc. Multimed.*, vol. 27, no. 2, pp. 125–140, 2016.

[9] K. Vallejo, L. Alarcón, and L. Ortegón, "Exploración del diseño y arquitectura web. Aplicación a páginas electrónicas del sector bancario desde la perspectiva del usuario," *Rev. EAN*, no. 80, pp. 59–83, 2016.

[10] J. M. San and M. García, "La Seguridad de la Información."

[11] "¿Seguridad informática o seguridad de la información?" [Online]. Available: https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/. [Accessed: 16-Jun-2019].

[12] "Software ISO 27001 Sistemas de Gestión de Seguridad de la Información." [Online]. Available: https://www.isotools.org/software/riesgos-y-seguridad/iso-

27001. [Accessed: 09-Jun-2019].

[13] A. De Sistemas and A. De Sistemas, “La seguridad informática y la seguridad de la información Information security and information security Segurança da informação e segurança da informação,” vol. 2, no. 12, pp. 145–155, 2017.

[14] U. K. Singh, C. Joshi, and D. Kanellopoulos, “A framework for zero-day vulnerabilities detection and prioritization,” *J. Inf. Secur. Appl.*, vol. 46, pp. 164–172, 2019.

[15] Y. Wang and J. Yang, “Ethical hacking and network defense: Choose your best network vulnerability scanning tool,” *Proc. - 31st IEEE Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2017*, pp. 110–113, 2017.

[16] hackin9.org, “Seguridad en Redes,” *Segur. En Redes Telemat.*, 2015.

[17] E. B. De Souza and A. Fernandes, “Um dataset de ataques Low Rate DDoS.”

[18] N. Vlajic and D. Zhou, “IoT as a Land of Opportunity for DDoS Hackers,” *Computer (Long. Beach. Calif).*, vol. 51, no. 7, pp. 26–34, 2018.

[19] D. Arivudainambi, V. K. Varun, and S. Sibi Chakkaravarthy, “LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks,” *Neural Comput. Appl.*, vol. 7, pp. 1–11, 2018.

[20] L. Patricia and Z. Molina, “Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución,” 2012.

[21] S. G. B. B. Gupta, “XSS-SAFE : A Server-Side Approach to Detect and Mitigate Cross-Site Scripting (XSS) Attacks in JavaScript Code,” 2015.

[22] R. Baloch, *Ethical Hacking and Penetration Testing Guide*. Auerbach Publications, 2018.

[23] J. Chavarri, “Hardening — Asegurando Apache – Guayoyo – Medium.” [Online]. Available: https://medium.com/guayoyo/hardening-asegurando-apache-abc52f87d750. [Accessed: 09-Jun-2019].

[24] E. A. Varela-tapia and J. M. Yagual-lozano, “servers on the same platform servidores em um VoIP plataforma,” vol. 2, no. 6, pp. 516–541, 2017.

[25] L. Castro, M. Rodríguez, A. Vales, and I. E. Blanco Amor, “Sistemas Operativos,” 2016. [Online]. Available: https://www.edu.xunta.gal/centros/iesblancoamorculleredo/aulavirtual2/pluginfile.php/25655/mod_page/content/30/SistemasOperativos_LauraCastro_NoeliaPombo_AntiaVales.pdf. [Accessed: 27-Jun-2019].

[26] Barrios A, “Introducción al web,” in *Sección Informática*, 2016.

[27] D. Merkel, “Docker : Lightweight Linux Containers for Consistent Development and Deployment Docker : a Little Background Under the Hood.”

[28] S. Jajodia and C. Mazumdar, “Information Systems Security: 11th International conference, ICISS 2015 Kolkata, India, december 16–20, 2015 proceedings,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9478, pp. 501–510, 2015.

[29] D. Appelt, C. D. Nguyen, A. Panichella, and L. C. Briand, “A Machine-Learning-Driven Evolutionary Approach for Testing Web Application Firewalls,” *IEEE Trans. Reliab.*, vol. 67, no. 3, pp. 733–757, 2018.

[30] J. J. Singh, H. Samuel, and P. Zavarsky, “Impact of paranoia levels on the effectiveness of the modsecurity web application firewall,” *Proc. - 2018 1st Int. Conf. Data Intell. Secur. ICDIS 2018*, pp. 141–144, 2018.

[31] A. Balaz, N. Adam, E. Pietrikova, and B. Mados, “ModSecurity IDMEF module,” *SAMI 2018 - IEEE 16th World Symp. Appl. Mach. Intell. Informatics Dedic. to Mem. Pioneer Robot. Antal K. Bejczy, Proc.*, vol. 2018-Febru, pp. 43–48, 2018.

[32] “FAQ – OWASP ModSecurity Core Rule Set.” [Online]. Available: https://coreruleset.org/faq/. [Accessed: 28-Jul-2019].

[33] Acens, “Certificados de Seguridad,” 2015.

[34] “Política de Certificación de Certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV).”

[35] “Marco Legal del Software Libre en Ecuador – ASLE.” [Online]. Available: https://www.asle.ec/marco-legal-del-softwarelibre-en-ecuador/. [Accessed: 01-Aug-2019].

[36] A. I. V Nº, I. N. G. Hugo, and D. E. L. Pozo, “Social De Los,” p. 116, 2016.

[37] M. E. C. Hurtado, D. Javier, and A. Sarango, “Análisis de Certificados SSL / TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación . (Analysis of free SSL / TLS Certificates and their implementation as Security Mechanism in Application Servers .),” pp. 273–286, 2017.