UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad De Ingeniería Civil, De Sistemas Y De Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OPTAR EL TITULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

TITULO

Prototipo de Detección Y Mitigación de Ataques de Denegación de Servicios (DoS), en Servidores Web

PRESENTADO POR

Bach. YESQUEN RODRIGUEZ RANDY STEVE

ASESOR

Mg. Ing. JUAN ELIAS VILLEGAS CUBAS

LAMBAYEQUE – PERÚ

MARZO 2018

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad De Ingeniería Civil, De Sistemas Y De Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Prototipo de Detección Y Mitigación de Ataques de Denegación de Servicios (DoS) en Servidores Web

RESPONSABLE

_____

Bach. YESQUEN RODRIGUEZ RANDY STEVE

ASESOR

_____

Mg. Ing. JUAN ELIAS VILLEGAS CUBAS

Sustentada y Aprobada ante el distinguido Jurado

_____

M. A. Ing. Robert Puican Gutiérrez
Presidente del Jurado

_____ _____

M. Sc. Ing. Martin Ampuero Pasco
1er Miembro del Jurado

Ing. César Guzmán Valle
2do Miembro del Jurado

LAMBAYEQUE – PERÚ

MARZO 2018

DEDICATORIA

"A mis padres y mis hermanos por ser los pilares fundamentales en mi vida, en mi educación profesional y moral, por su apoyo incondicional desmedido y la motivación que siempre me brindaron.
Todo este trabajo ha sido posible gracias a ellos"

AGRADECIMIENTOS

"A Dios por acompañarme siempre y guiarme a lo largo de mi carrera profesional, por haberme permitido llegar tan lejos y hacer realidad mi sueño más anhelado".

"Al Ing. Juan Villegas Cubas por compartir sus conocimientos conmigo, por brindarme su amistad y confianza, por tener la paciencia para guiarme y resolver mis dudas durante el desarrollo de mi investigación".

"A mis tíos Wilmer y Yescenia por su apoyo constante, por los consejos que me brindaron, por su cariño infinito hacia m"í.

"A Patty, Daniel, Joao, que de una u otra manera me ayudaron a construir esta investigación, por su apoyo incondicional, a cualquier hora y lugar".

RESUMEN

Un ataque de Denegación de Servicio (DoS) es un tipo de ataque que tiene por finalidad que un servicio o recurso sea inaccesible a los usuarios legítimos por un periodo de tiempo indeterminado, generando así perdidas de distintos tipos por la indisponibilidad de los servicios prestados, esto es muy perjudicial para las diferentes empresas que tienen vida en internet.

La mayoría de veces las pequeñas empresas no tienen los recursos económicos necesarios para implementar un buen servidor a nivel de hardware, por lo que se usa mejor un software que funciona en un ordenador convencional, estos equipos no son robustamente adecuados para soportar muchas peticiones de los distintos usuarios, por lo que son altamente vulnerables a los ataques de Denegación de Servicio.

Por tal motivo el objetivo de este proyecto es desarrollar un prototipo que detecte y mitigue los ataques DoS que sufren los servidores Web para mantener la disponibilidad de los servicios ofrecidos por el servidor y que sea menos costoso y más efectivo que algunos de los prototipos ya propuestos anteriormente.

La presente investigación utiliza apache como plataforma para los servicios de servidor web ejecutado bajo el sistema operativo Linux Ubuntu por ser libre y sin costo por licencia, posteriormente se hace una comparación con otra propuesta de solución que tiene la misma finalidad que la presente investigación, pero con diferentes mecanismos de defensa, pudiendo probar al final de todo el desarrollo de la investigación cuál de las dos soluciones propuestas es más efectiva contra los ataques DoS.

ABSTRACT

A Denial of Service (DoS) attack is a type of attack that aims to make a service or resource inaccessible to legitimate users for an indeterminate period of time, thus generating losses of different types due to the unavailability of the services provided, This is very harmful for the different companies that have life on the internet.

Most times small businesses do not have the financial resources to implement a good server at the hardware level, so software that works on a conventional computer is better used, these computers are not robustly suited to support many requests from different users, so they are highly vulnerable to Denial of Service attacks.

For this reason the objective of this project is to develop a prototype that detects and mitigates the DoS attacks suffered by Web servers to maintain the availability of the services offered by the server and that is less expensive and more effective than some of the prototypes already proposed. previously.

The present research uses apache as a platform for web server services run under the Linux Ubuntu operating system because it is free and free of charge, then a comparison is made with another solution proposal that has the same purpose as the present investigation but with different defense.

INDICE

Índice de Figuras

Índice de Tablas

INTRODUCCIÓN

A medida que evolucionan las soluciones tecnológicas, también evolucionan los mecanismos de guerra informática que atentan contra la seguridad de las plataformas informáticas. Uno de los ciberataques más tradicionales se hace a través del método de denegación de servicio (DoS). Esta técnica se inicia en el año 2000, pero en estos últimos años se ha visto el crecimiento en el uso, logrando dejar fuera de servicio grandes soluciones informáticas en el mundo.

En la actualidad los Ataques de Denegación de Servicio (DoS) vienen siendo usados frecuentemente porque en muchos de los casos no requiere conocimientos avanzados de seguridad informática como otros tipos de ataques. Es por ello que estos tipos de ataques se han convertido en un recurso bastante habitual para los hackers, incluso para aquellas personas que recién están entrando en el mundo de la informática.

Estas características convierten a los ataques DoS en una gran amenaza para cualquier negocio, sobre todo para aquellos negocios que dependen de su página web en internet porque por medio de esta generan distintas operaciones en tiempo real, por lo que un ataque DoS que los deje fuera de servicio originaria muchas pérdidas.

CAPITULO I: PROBLEMA DE LA INVESTIGACIÓN

1.1. SITUACION PROBLEMÁTICA

En estos últimos años el acceso al internet y a sus servicios se ha convertido en la acción más habitual de las personas desde cualquier hogar o centro laboral, somos muchos los que frecuentemente utilizamos nuestro navegador para buscar información, hacer transacciones o pagos online, comprar por Internet o, simplemente, para echar un vistazo a la prensa diaria a través de internet.

Las organizaciones, independientemente de su tamaño, dispone de su página web para divulgar por Internet su negocio, su identidad, su imagen; desde la página solo informativa, hasta la que cuenta con capacidad para realizar operaciones dentro de ella y dar un servicio directo a los usuarios de la misma.

Netcraft en sus informes de seguridad, dio a conocer las cifras actuales que registra la Red. Según el informe, “en el mundo ya hay 1,436,724,046 de sitios web”.

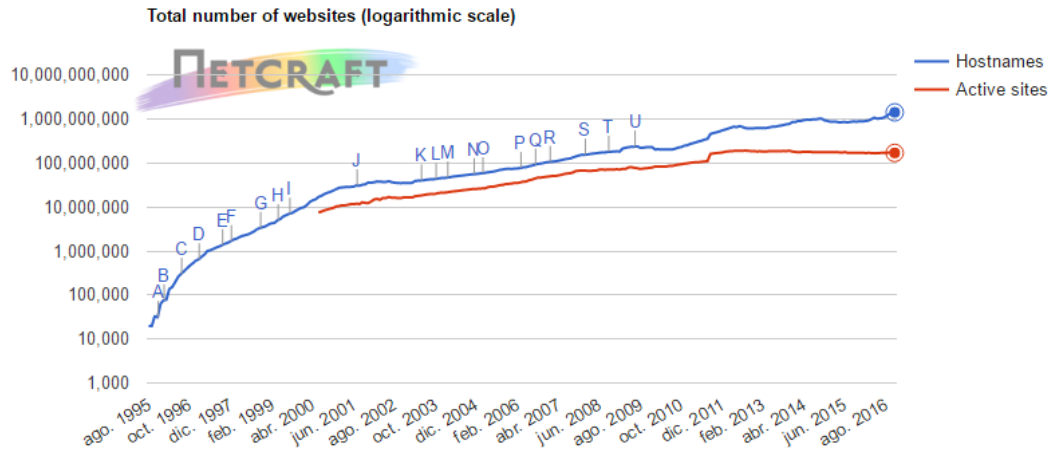


Figura 1 Crecimiento de los sitios web en la actualidad

Fuente: NETCRAFT

Un sitio web está alojado en un servidor web. Ahora bien, un servidor web es un programa que se ejecuta continuamente en un dispositivo, manteniéndose a la espera de peticiones que le hará el cliente, luego se encarga de contestar a estas peticiones entregando como resultado una página web; los servidores web están especialmente preparados para estar en funcionamiento los 365 dias del año.

Los servidores web quedas expuestos a internet y pueden sufrir miles de ataques que tratan de acceder a tus datos, utilizar tu página para propagar archivos maliciosos, servir publicidad intrusiva o simplemente dejar fuera de servicio a la página.

En la figura 2, se muestra el reporte de SECURI sobre la seguridad de los sitios web y las principales vías de los ciberdelincuentes para tratar de romper las barreras de seguridad de los servicios de creación de páginas web más utilizados, como WordPress, Joomla, Drupal o Magento.

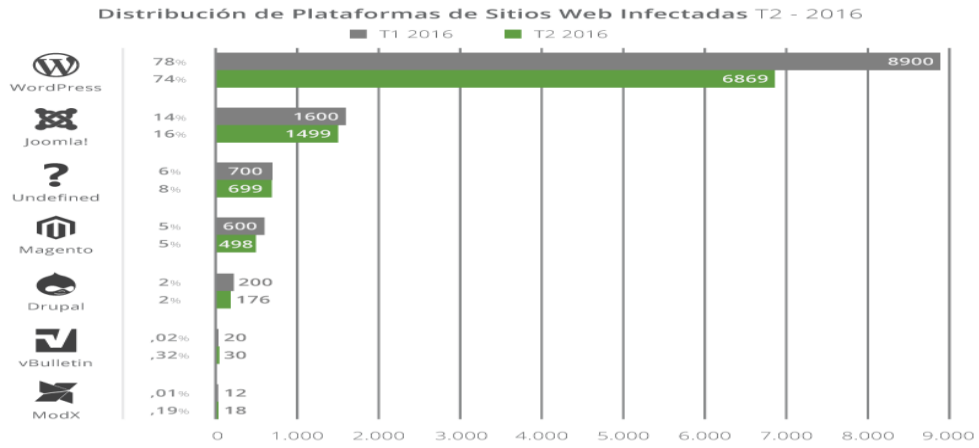


Figura 2 Reporte de SECURI (Informe de sitios web hackeados 2016-T2)

Según este estudio, los principales problemas de seguridad detectados han sido: Cross Site Scripting (XSS), Fuerza bruta, Inyección de código SQL y la denegación de servicio.

Los ataques de Denegación de Servicio (DoS) entre ellos el ataque DDoS (Ataque de denegación de servicio distribuido) que es un tipo de ataque DoS, están en aumento y se han convertido en desafíos de seguridad complejos y abrumadores para las organizaciones grandes y pequeñas.

Figura 3 Ataques DoS en tiempo real según NorseCorp

Según el informe emitido por Kaspersky LaB que tiene años de experiencia en la lucha contra las amenazas cibernéticas, entre ellas los ataques DoS de diversos tipos y grados de complejidad.

En la figura 4, se muestra que en el 2016 se registraron ataques DoS en 70 países, el 77,4% corresponde a China. En general, el 97,3% de los ataques afectó al TOP 10 de países.

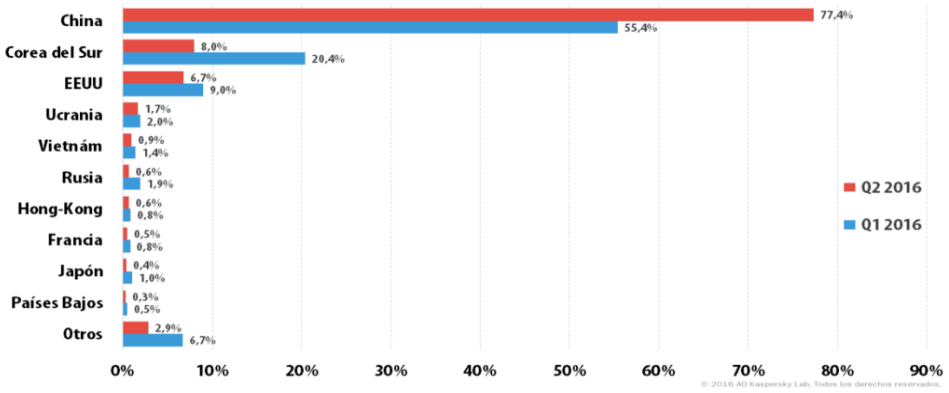


Figura 4 Distribución de blancos únicos de ataques DDoS por país

El último incidente de un tipo de ataque DoS ocurrió en el ciberataque a Dyn que tuvo lugar el 21 de octubre de 2016 y se basó en múltiples ataques de denegación de servicio a sistemas operados por el proveedor de nombres de dominio (DNS, por sus siglas en inglés).

De acuerdo con investigadores de Flashpoint, una compañía de seguridad informática, el ataque provino de una botnet basada en Mirai. Botnet es el término que se usa para referirse a una red de bots que se ejecutan de manera autónoma y automática; por otra parte Mirai es un software malicioso capaz de lanzar ataques masivos a través de dispositivos conectados a internet.

A pesar de que los ataques DoS no son un fenómeno reciente, los métodos y los recursos disponibles para llevarlos a cabo y las técnicas para enmascarar los han evolucionado dramáticamente, con todo esto, los servidores web han pasado a ser un blanco preferido para cualquier tipo de ciberdelincuente.

1.2. FORMULACION DEL PROBLEMA

¿Cómo detectar y mitigar los ataques DoS en los servidores web?

1.3. JUSTIFICACION DE LA INVESTIGACION

- **Aporte Práctico**

  Esta investigación tiene como objetivo mejorar la resistencia de los Sistemas de Información de las pequeñas empresas, a los ataques de denegación de servicio a los que puedan verse expuestos, a partir de la incorporación de elementos de software libre para combatir de la forma más efectiva dichos ataques, incurriendo en bajo costo por el hecho de usar software libre.

- **Relevancia Social**

  El presente trabajo de investigación pretende beneficiar al micro y pequeña empresa que quieran proteger sus servicios web de los ataques de denegación de servicio y que no tengan los recursos suficientes para poder comprar soluciones en equipos (hardware) como firewall, IDS, IPS, etc. Disminuyendo los costos y haciendo un mejor uso de los recursos con los que cuenta la empresa que quiera implementar el modelo propuesto.

1.4. LIMITACIONES DE LA INVESTIGACIÓN

- Se usará máquinas virtuales y PC físicas con sistema operativo Windows y Linux.
- El desarrollo del prototipo se realizará dentro de un laboratorio propio, utilizando herramientas para publicar nuestra web en internet y así cualquier usuario pueda acceder a la página web.
- Se usará Apache como servidor web por que el 46% de los servidores en el mundo usan apache como plataforma web según el último informe emitido por Netcraft en el mes de noviembre del 2016.
- El servidor web se encuentra dentro de una DMZ (Zona Desmilitarizada)
- Se utilizará el tipo de ataque DoS basados en volumen, usando la herramienta HTTP Attack.

- No se implementó en una empresa por que las pruebas que se tenían que hacer podrían dejar fuera de servicio más de una vez la plataforma web de la empresa.

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. OBJETIVO GENERAL

- Implementar y evaluar un prototipo con mecanismos de seguridad para la detección y mitigación de ataques de denegación de servicio en servidores web.

1.5.2. OBJETIVOS ESPECIFICOS

- Identificar los tipos de ataques de denegación de servicios en servidores web.

- Identificar y analizar los mecanismos de protección contra los ataques DoS en servidores web.

- Implementar un prototipo de mitigación de ataques DoS con los mecanismos analizados.

- Evaluar el prototipo implementado para verificar la efectividad ante los ataques DoS.

CAPITULO II: MARCO TEORICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Antecedente N° 1

Título	Esquema de seguridad contra ataques DoS y DDoS, Caso: Diario de Quintana Roo
Universidad	Universidad de Quintana ROO
Fecha	2013
Autor(es)	Rogelio Armando Tello Padilla
Análisis de relación con la presente investigación	Este trabajo se relaciona con la investigación porque utiliza herramientas de mitigación de ataques DoS para mejorar la disponibilidad de un sitio web.

Antecedente N° 2

Título	Prototipo de detección de ataques distribuidos de denegación de servicios (DDoS) a partir de máquinas de aprendizaje
Universidad	Universidad Autónoma de Manizales
Fecha	2015
Autor(es)	Manual Sebastián Hoyos Llanos
Análisis de relación con la presente investigación	Este trabajo se centra en lo que es detección de ataques DoS a partir de ciertos mecanismos de aprendizaje para luego tratar de reducir su impacto.

Antecedente N° 3

Título	Una arquitectura distribuida para la detección, comunicación y mitigación de la denegación de servicio
Universidad	Universidad Rey Juan Carlos
Fecha	2013
Autor(es)	Luis Campo Giralte
Análisis de relación con la presente investigación	Este trabajo se relaciona con la investigación porque combina la detección, comunicación y posteriormente la mitigación de los ataques DoS, en el orden mencionado para poder cumplir sus objetivos con respecto a los ataques DoS.

Antecedente N° 4

Título	Ataques de Denegación de Servicio a baja tasa contra servidores
Universidad	Universidad de Granada
Fecha	2007
Autor(es)	Gabriel Macia Fernández
Análisis de relación con la presente investigación	Este trabajo nos muestra cómo se ejecutan los ataques DoS y cómo funcionan generalmente los mecanismos de defensa que los tratan de eliminar, nos muestra el punto de vista de un atacante.

Antecedente N° 5

Título	Extracción de datos para la clasificación y filtrado de IPs falsas en ataques DDoS
Universidad	Universidad Nacional Abierta y a Distancia (UNAD)
Fecha	2013
Autor(es)	Yudy Angelica Ramírez Walteros
Análisis de relación con la presente investigación	En este proyecto nos ayuda a identificar las direcciones IP falsas mediante una captura de tráfico para su posterior análisis para luego saber diferencias entre un IP legitima que realiza peticiones comunes al servidor o una IP falsa que lo único que busca es saturar los recursos de este.

Antecedente N° 6

Título	Sistema detector de intrusiones ocupando una red neuronal artificial
Universidad	Universidad Autónoma del Estado de México
Fecha	2015
Autor(es)	José Ernesto Luna Domínguez
Análisis de relación con la presente investigación	Esta investigación nos muestra como la inteligencia artificial es útil para la detección de intrusos mejorando así el rendimiento de un IDS, para poder detectar y hasta predecir un ataque.

2.2. BASE TEÓRICA

2.2.1. Servidor

El término servidor tiene dos significados en el ámbito informático.

- **Servidor (hardware):** es una máquina física integrada en una red informática en la que, además del sistema operativo.
- **Servidor (software):** es un programa que ofrece un servicio especial que otros programas denominados clientes pueden usar a nivel local o a través de una red.

2.2.2. Tipos de Servidores

En esta tabla podemos ver los tipos de servidores más habituales.

DENOMINACIÓN	DESCRIPCIÓN
Servidor de Correo	Es el servidor que almacena, envía, recibe y realiza todas las operaciones relacionadas con el e-mail de sus clientes.
Servidor Proxy	Es el servidor que actúa de intermediario de forma que el servidor que recibe una petición no conoce quién es el cliente que verdaderamente está detrás de esa petición.
Servidor Web	Almacena documentos HTML, imágenes, videos, texto, presentaciones, y en general todo tipo de información.
Servidor de Base de Datos	Da servicios de almacenamiento y gestión de bases de datos a sus clientes. Una base de datos es un sistema que nos permite almacenar grandes cantidades de información.
Servidores Clúster	Son servidores especializados en el almacenamiento de la información teniendo grandes capacidades de almacenamiento y permitiendo evitar la pérdida de la información por problemas en otros servidores.
Servidores Dedicados	Como ya expresamos anteriormente, hay servidores compartidos si hay varias personas o empresas usando un mismo servidor, o dedicados que son exclusivos para una sola persona o empresa.
Servidores de imágenes	Recientemente también se han popularizado servidores especializados en imágenes, permitiendo alojar gran cantidad de imágenes sin consumir recursos de nuestro servidor web, en almacenamiento o para almacenar fotografías personales, profesionales, etc.

Tabla 1 Tipos de Servidores

Fuente: Elaboración Propia

2.2.3. Servidor Web

Es un programa que gestiona cualquier aplicación en el lado del servidor realizando conexiones bidireccionales y/o unidireccionales, síncronas o asíncronas con el cliente generando una respuesta en cualquier lenguaje o aplicación en el lado del cliente. El código recibido por el cliente suele ser compilado y ejecutado por un Navegador Web.

Para la transmisión de todos estos datos se utiliza algún protocolo. Generalmente se utiliza el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del Modelo OSI.

2.2.4. ¿Cómo funciona el servidor web?

Las páginas web se visualizan en un explorador web como Google Chrome y se almacenan en Servidores Web.

Cuando nosotros accedemos a un sitio web como por ejemplo a al sitio de la UNPRG, introducimos una URL en nuestro navegador (“www.unprg.edu.pe”) lo que estamos haciendo en realidad es una solicitud o petición de una página web a un servidor web; y éste busca el archivo (página web) que el cliente a solicitado y finalmente devuelve la página en un código en específico y ésta es interpretada en el navegador web.

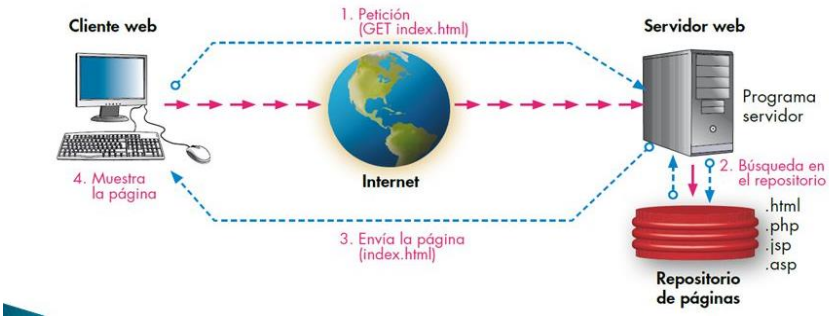
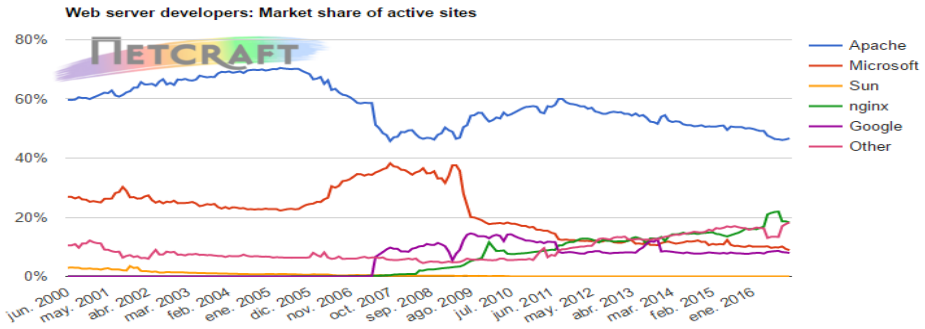


Figura 5 Proceso de visita de un usuario a un sitio web

Fuente: SecureList

2.2.5. Servidores web más usados

Según el último informe emitido por Netcraft en el mes de noviembre del 2016 los servidores web más populares actualmente son Apache, Microsoft IIS, Sun Java System Web, Ngnix y Lighttpd.



Developer	October 2016	Percent	November 2016	Percent	Change
Apache	82,052,688	46.30%	80,012,251	46.67%	0.37
nginx	32,968,259	18.60%	31,239,615	18.22%	-0.38
Microsoft	16,434,903	9.27%	15,257,724	8.90%	-0.37
Google	14,396,867	8.12%	13,607,864	7.94%	-0.19

Figura 6 Servidores web más usados actualmente

Fuente NETCRAF

2.2.6. Tipos de Ataques a Servidores web

2.2.6.1. SQL INJECTION (SQLI)

Los ataques de SQL inyección, se consideran una técnica para alterar una cadena de consulta a una base de datos, inyectando código en la consulta; tratando de acceder a información no autorizada almacenada en la base de datos.

2.2.6.2. Fuerza Bruta

Estos son básicamente intentar "**romper**" todas las combinaciones posibles de nombre de usuario + contraseña en una página web.

2.2.6.3. Cross Site Scripting (XSS)

XSS es considerado un estilo de ataque en el que la parte delantera de la página web actúa como un punto de lanzamiento para ataques a otros usuarios que visitan el sitio web.

2.2.6.4. DoS – DDoS (Denegación de Servicio – Denegación de Servicio Distribuido)

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.

2.2.7. Tipos de Ataque DoS

Según la empresa SECURI hay tres tipos de ataques DoS.

1. **Ataques DoS Basados en Volumen**

   En este tipo de ataque gana el que tiene más recursos entre el servidor y el dispositivo (o dispositivos) del atacante. Los atacantes tratan de interrumpir los servicios de un servidor consumiendo los recursos de éste.

2. **Ataques DoS Basados en Protocolos**

   Los atacantes hacen uso de las debilidades de los protocolos en los que se basa el funcionamiento del internet, como ping, SYN Flood, modificación de los paquetes IP entre otros para dejar fuera de servicio a un servidor web.

3. **Ataques en la Capa de Aplicación**

   Cuando el atacante aprovecha vulnerabilidades de las aplicaciones de los servidores web como IIS, apache; y también a plataformas de aplicaciones como WordPress, Joomla y otras aplicaciones similares.

2.2.8. Principales Ataques DoS

Según (Britos, 2010) los principales ataques son:

1. **Ataque Smurf**

   “Normalmente se utilizan paquetes ICMP. La red sirve entonces como un smurf amplificador. En ese ataque, los atacantes envían un gran número de paquetes IP con la dirección de la fuente falsa, en la dirección de la fuente se coloca la dirección de la víctima”.

2. **Inundaciones Ping**

   “Se basa en el envío a la víctima un número muy grande de paquetes ping, por lo general a través del comando ping - f”.

3. **Inundación TCP-SYN**

   “Los ataques más comunes de DoS, se produce cuando se establece una conexión Internet, con el protocolo de TCP desde un cliente a un servidor y el cliente envía un paquete de sincronización (SYN), el servidor responde con un paquete de reconocimiento de sincronización (SYN ACK), esperando el reconocimiento del cliente (ACK).”

4. **Ataque Teardrop**

   “El ataque consiste en el envío de paquetes IP fragmentados de tal forma que los fragmentos se superpongan, provocando sobrecargas en la computadora de destino. Los elementos manejados son la superposición de fragmentos, más el tamaño grande de estos provocan sobrecarga en la computadora de destino”.

5. **Ataques Peer-to-peer**

   “El más agresivo de estos ataques DDoS peer-to-peer, los ataques Peer-to-peer son diferentes de los ataques basados en botnet (botnet es un término usado para designar una colección de programas robots (bots) los cuales pueden ser ejecutados de manera autónoma y en forma automática”.

6. **Inundaciones a nivel de Aplicación**

   “Inundaciones IRC (Internet Relay Chat) constituye un ataque común a nivel de aplicación. Varios DoS exploits causan desbordamiento de buffer que pueden provocar que el software que se está ejecutando en el servidor llene el espacio en el disco o consuma toda la memoria o tiempo de CPU”

7. **Ataque Zombie**

   “Una red es objeto de hostilidad por diferentes atacantes haciendo ping a las computadoras durante un largo período de tiempo”.

8. **Ataque Nuke**

   “Nuke es un viejo ataque de denegación de servicio contra las redes que consiste en el envío de paquetes ICMP fragmentados o paquetes ICMP inválidos esto se logra mediante una modificación a la utilidad ping que provoca el envió repetido de datos corruptos, provocando ralentizar la computadora afectada, hasta que llega a un alto total”.

9. **Ataques distribuidos**

   “Un ataque distribuido de denegación de servicio (DDoS) se produce cuando varios sistemas generan una inundación comprometiendo el ancho de banda o recursos de un sistema, por lo general uno o más servidores web”.

   Las principales ventajas para un atacante de la utilización de un ataque de denegación de servicio distribuido es que múltiples máquinas que pueden generar más tráfico que un ataque de la máquina, múltiples máquinas de ataque son más difíciles de apagar que el ataque de una sola máquina, y que el comportamiento de cada máquina de ataque, pueden ocultarse mejor, lo que lo hace más difícil de detectar y evitar

2.2.9. Herramientas de Ataque DoS

Según (Hoyos Llanos, 2015) las principales herramientas de ataque DoS son

1. **LOIC (Low Orbit Ion Canon)**

   "LOIC es una de las herramientas más populares de DOS disponibles en Internet. Se puede utilizar simplemente por un solo usuario para llevar a cabo un ataque DoS en servidores pequeños"

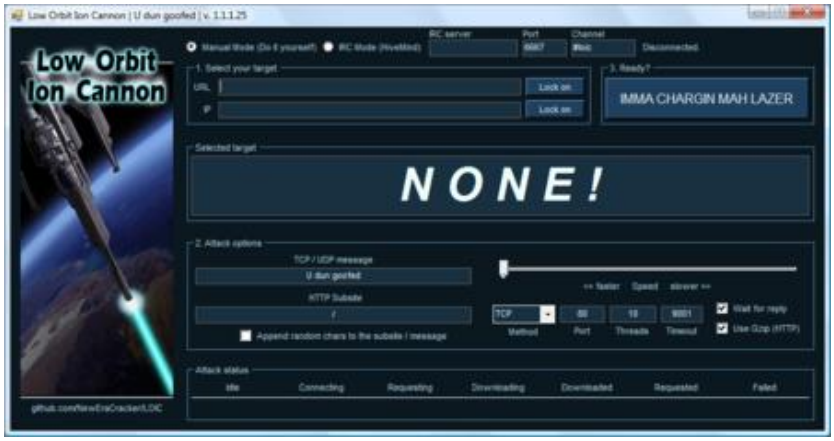


Figura 7 Interface de software LOIC

Fuente: https://www.incapsula.com/ddos

2. **XOIC**

   "XOIC es otra buena herramienta atacar DoS. Se lleva a cabo un ataque DoS un cualquier servidor con una dirección IP, un puerto seleccionado por el usuario, y un protocolo seleccionado por el usuario".

Figura 8 Interface de software XOIC

Fuente: https://www.incapsula.com/ddos

3. HULK (HTTP Unbearable Load King)

"HULK genera una solicitud única para todos y cada solicitud generada al tráfico ofuscado en un servidor web. Esta herramienta utiliza muchas otras técnicas para evitar la detección de ataques a través de patrones conocidos".

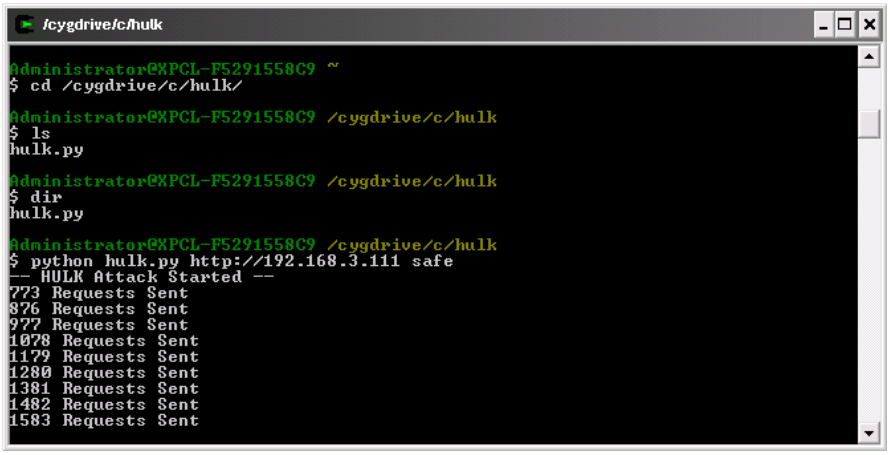


Figura 9 Interface de software HULK

Fuente:http://www.sectorix.com/2012/05/17/hulk-web-server-dos-tool/

4. DDOSIM-Layer 7 DDOS Simulador

"Se utiliza para llevar a cabo ataques DDoS mediante la simulación de varios ejércitos de zombies (ordenadores infectados). Todos los ejércitos de zombies crean conexiones TCP completas al servidor de destino".

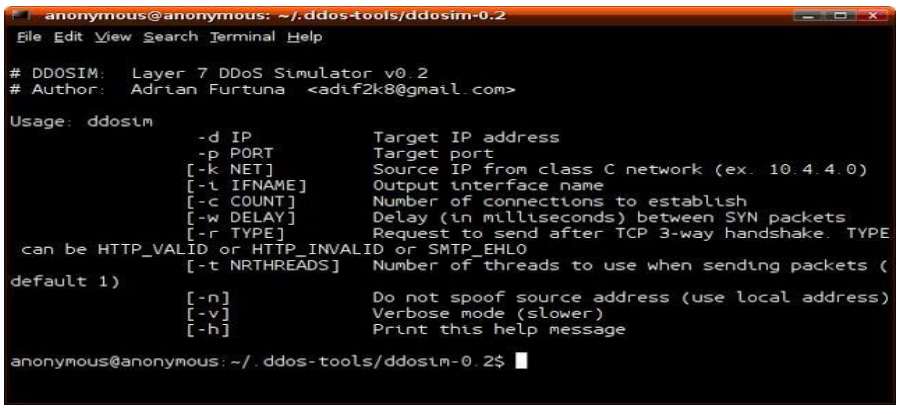


Figura 10 Interface de software DDOSIM-Layer 7 DDOS Simulador

Fuente: https://www.incapsula.com/ddos

5. HTTP ATACK

"Se realiza un ataque DOS con el envío de datos desde un formulario WEB mediante el método POST. Esta herramienta viene con un menú en la consola interactiva".

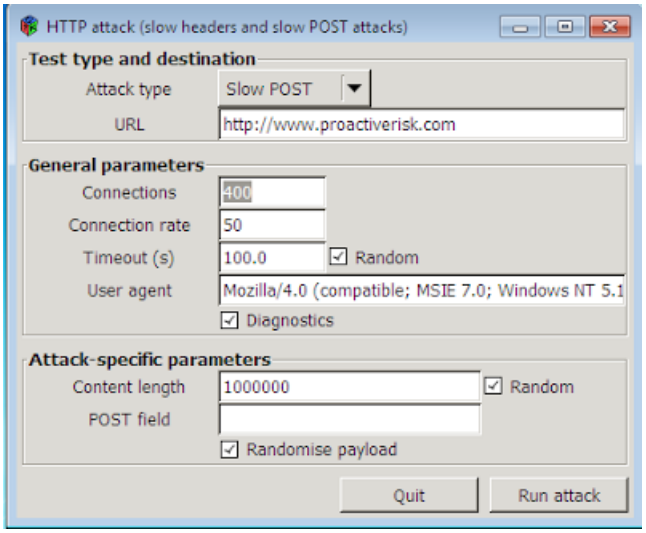


Figura 11 Interface de software HTTP ATTACK

Fuente: https://www.incapsula.com/ddos/attack-glossary/http-flood.html

6. Tors Hammer:

"Es una herramienta desarrollada en Python y se puede ejecutar a través de una red TOR y ser anónimo mientras se realiza el ataque. Es una herramienta eficaz que puede matar a los servidores Apache o IIS en pocos segundos"

Figura 12 Interface de software Tors Hammer

Fuente: Elaboración Propia

7. **Pyloris**

"Con esta herramienta se pueden utilizar servidores proxy SOCKS y conexiones SSL para realizar un ataque DOS en un servidor"

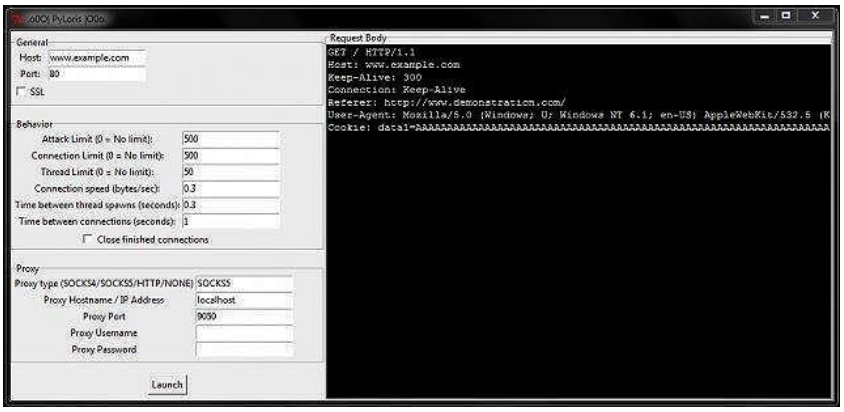


Figura 13 Interface de software Pyloris

Fuente: Elaboración Propia

2.2.10. Detección de ataques DoS

La detección de los ataques se puede realizar basado en firmas y basado en anomalías.

2.2.10.1. Detección de ataques DoS basados en firmas

Los mecanismos de detección de ataques de denegación de servicio basados en firmas almacenan patrones de ataque (firma) en una base de datos.

2.2.10.2. Detección de ataques DoS basados en anomalías

Los mecanismos que utilizan detección de anomalías se basan en la existencia de una caracterización del comportamiento normal o anormal de un sistema, de modo que su funcionamiento en un instante determinado puede ser comparado con el modelo existente para determinar si se está produciendo o no una anomalía.

2.2.11. Sistema de Detección de Intrusos (IDS)

El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

2.2.11.1. Funcionamiento de un IDS

El funcionamiento de un IDS, se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas, o comportamientos sospechosos para clasificar a un tráfico como intrusión o normal.

2.2.11.2.Tipos de IDS

a) NIDS

Analiza el segmento de red, capturando y analizando los paquetes que son transmitidos en la red.
Para que los NIDS sean efectivos, han de ser actualizados periódicamente.

- **SNORT**
  Snort es un sistema libre y abierto de red de fuente de prevención de intrusiones y la red del sistema de detección de intrusos (NIDS).

Figura 14 Icono Snort

Fuente: https://www.snort.org/

- **SURICATA**

  Suricata es un motor de detección de amenazas de red libre, maduro, rápido y sólido de fuente abierta y gratuita.

Figura 15 Icono Suricata

b) HIDS

Protege un único ordenador, monitorizando los eventos locales y analizando información del sistema mediante ficheros logs. Este IDS trabaja con la información recogida dentro de un solo host. Por ello, es necesario tener un HIDS en cada host que queramos monitorizar.

- **OSSEC**

  Es un HIDS que permite analizar los archivos logs, permite controlar la integridad de archivos y detectar rootkits, entre sus principales funcionalidades.

Figura 16 Icono OSSEC

- **TRIPWIRE**

  Es un HIDS que permite comprobar de forma diaria si se han realizado cambios en el sistema de archivos.

Figura 17 Icono Tripwire

2.2.12. Mitigación de ataques DoS

La mitigación se refiere al proceso que se realiza después que el ataque ha sido detectado. Y consiste en la ejecución de medidas que reduzcan en impacto de los daños ocasionados por el ataque.

2.2.12.1. Control de Trafico

El control de tráfico en la primera medida que se realiza a un ataque DoS, y consiste en eliminar todo el tráfico del ciberdelincuente.

2.2.12.2. Rastreo del ataque

El rastreo del ataque es otra medida de mitigación que tiene tres propósitos principales: el primero es identificar el tráfico de los ciberdelincuentes que están ejecutando el ataque DoS, luego se trata de conseguir a identificación del atacante y finalmente se obtiene información para hacer el control de tráfico.

2.2.12.3. Diferenciación de servicios (QoS)

Las técnicas de mitigación de diferenciación de servicios o Calidad de servicio (QoS – Quality of Service) priorizan el tráfico de unos servicios frente a otros, cuando la demanda excede a la oferta de tráfico.

2.3. DEFINICIONES DE TÉRMINOS TÉCNICOS

- **Prototipo:**
  - “Modelo o maqueta del sistema que se construye para comprender mejor el problema y sus posibles soluciones”
- **Ping:**
  - “Ping es una de las herramientas de diagnóstico más utilizadas en la administración de redes en todo el mundo”.
- **QoS**
  - “QoS (Quality of Service), o calidad de servicio, que establece diversos mecanismos destinados a asegurarnos la fluidez en el tráfico de la red”.
- **Malware**
  - “Es un código maligno, software malicioso, software dañino o software malintencionado, es un tipo de virus que tiene como objetivo infiltrarse o dañar un sistema”
- **Botnet**
  - “Botnet es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática”.
- **Zombies**
  - “Zombi es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de malware, pueden ser usados por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo”
- **TCP**
  - “Es un conjunto de reglas o normas que determinan cómo se realiza el intercambio de datos entre dos ordenadores”.
- **HTTP**
  - “Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. HTTP es un protocolo sin estado, es decir, no guarda ninguna información sobre conexiones anteriores”

CAPITULO III: MARCO METODOLÓGICO

3.1. TIPO Y DISEÑO DE LA INVESTIGACIÓN

3.1.1. TIPO DE LA INVESTIGACIÓN

A) De acuerdo con el fin que se persigue

- Aplicada

  - Guarda íntima relación con la básica, pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos.
  - La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar.

B) De acuerdo a la metodología para demostrar la hipótesis

- Experimental

  - La investigación experimental consiste en la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o por que causa se produce una situación o acontecimiento en particular.

  - Se trata de un experimento porque precisamente el investigador provoca una situación para introducir determinadas variables de estudio manipuladas por él, para controlar el aumento o disminución de esa variable, y su efecto en las conductas observadas. El investigador maneja deliberadamente la variable experimental y luego observa lo que sucede en situaciones controladas.

3.2. POBLACION Y MUESTRA

3.2.1. POBLACION

- La población es infinita debido a que la cantidad de ataques DoS pueden ser de un tamaño desconocido

3.2.2. MUESTRA

- Como la población es desconocida se utilizará la fórmula de obtención de muestra para una población infinita

$$n = \frac{z_{\alpha}^{2} * p * q}{e^{2}}$$

Donde:

n = tamaño de la muestra

Z = nivel de confianza

p = probabilidad a favor

q = probabilidad en contra

e = error muestral

Se desea estimar la proporción de ataques DoS se debe ejecutar para comprobar el prototipo de detección y mitigación de ataques DoS en servidores web, con una confianza del 95% y un error del 5%

Confianza 95% → Z = 1.96

Confianza	90%	91%	92%	93%	94%	95%	96%	97%	98%	99%
Z	**1.64**	**1.70**	**1.75**	**1.81**	**1.88**	**1.96**	**2.05**	**2.17**	**2.33**	**2.58**

Tabla 2 Niveles de confianza

Fuente: Elaboración Propia

P es la probabilidad de que ocurra el suceso esperado y como no hay una encuesta anterior o información previa se considerará

p = q = 0.5

Desarrollo:

$$n = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2}$$

$$n = 384.16 \rightarrow 385$$

Interpretación:

"Si se desea estimar los ataques DoS que se necesita para comprobar el funcionamiento del prototipo y se espera un resultado confiable del 95%, con un error del 5% se debería tomar una muestra de 385 ataques DoS".

3.3. HIPOTESIS

- El prototipo de detección y mitigación de ataques DoS reducirá el impacto que estos ataques tienen en los servidores web.

3.4. VARIABLES

3.4.1. VARIABLES DEPENDIENTES

- Prototipo de Detección y Mitigación de Ataques DoS

3.4.2. VARIABLES INDEPENDIENTES

- Impacto de los ataques DoS en servidores web

3.5. OPERACIONALIZACION

Miguel De la Hoz Correa (2016) menciona:

"Esas métricas son verdadero positivo (VP – ataque correctamente identificado como ataque), verdadero negativo (VN – tráfico normal correctamente identificado como tráfico normal), falso positivo (FP - tráfico normal identificado incorrectamente como ataque) y falso negativo (FN - ataque identificado incorrectamente como tráfico normal)." (p.36).

Los indicadores que emplearemos durante el desarrollo de la tesis serán los verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos, también la disponibilidad de tiempo que el servidor está atendiendo las peticiones de los usuarios

INDICADOR	ECUACIÓN	PREGUNTA	ESCALA
Disponibilidad del Servicio	[(Verdaderos Negativos) *100]	¿Cuál es el porcentaje de peticiones legitimas son atendidas por el servidor	0 – 100%
Tasa de Verdaderos Positivos (VP)	[(Número de Ataques detectados) / (Número Total de pruebas)]*100	¿Cuál es el porcentaje de ataques correctamente detectados?	0 – 100%
Tasa de Verdaderos Negativos	[(Número de Tráfico Legítimo no Detectado como Ataque) / (Número Total de pruebas)] *100	¿Cuál es el porcentaje de tráfico legítimo que no es detectado como ataque?	0 – 100%
Tasa de Falsos Positivos	[(Número de tráfico Legítimo Detectado como Ataque) / (Número Total de Pruebas)]*100	¿Cuál es el porcentaje de tráfico legítimo que es detectado como ataque?	0 – 100%
Tasa de Falsos Negativos (FN)	[(Número de Ataques no Detectados) / (Número Total de Pruebas)]*100	¿Cuál es el porcentaje de ataques que no fueron detectados?	0 – 100%

Tabla 3 Operacionalización de las Variables

Fuente: Elaboración Propia

3.6. ESTRATEGIA PARA LA DEMOSTRACION DE LA HIPOTESIS, TECNICAS E INSTRUMENTOS DE RECOLECCION DE DATOS

3.6.1. ESTRATEGIA PARA LA DEMOSTRACION DE LA HIPOTESIS

Para demostrar la hipótesis planteada en el punto 3.3, se utilizará un diseño PreTest y un diseño PostTest en dos grupos diferentes, de tal manera que con los resultados obtenidos podamos medir cuál de los dos mecanismos de protección es mejor frente al tipo de ataque DoS que vamos a realizar mediante la herramienta HTTP Attack.

El número de veces que realizaremos las pruebas será de acuerdo al punto 3.22 de esta investigación, con la máxima cantidad de conexiones que nos permita el software de ataques DoS

Para un diseño propiamente experimental tendríamos la siguiente figura

Grupo	*Asignación*	*Pretest*	*Tratamiento*	*Posttest*
A	sí R	O	X	O
B	sí R	O		O

Figura 18 Diseño Experimental

Fuente:http://www.postgradoune.edu.pe/documentos/Experimental.pdf

Siendo:

- R: Azar
- O: Observación
- X: Variable Independiente

Según (Murillo, 2012), “este diseño es de los más completos que se pueden usar en investigación experimental, pues al incorporar un grupo de control que tiene las mismas experiencias que el grupo experimental, excepto el tratamiento, la validez interna queda asegurada”.

3.6.2. TECNICAS DE RECOLECCION DE DATOS

a) Observación

La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos.

- **Observación Directa y/o Participante:** “Cuando el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar”.

- **Observación Experimental:** “Es un procedimiento primordial de la investigación, es planificada, controlada, sujeta a comprobaciones, controles de validez y fiabilidad”.

- **Observación de laboratorio:** “Es la que se realiza en lugares pre-establecidos, con grupos humanos previamente determinados”.

- **Observación de equipo o de grupo**: “Es la que se realiza por parte de varias personas que integran un equipo o grupo de trabajo que efectúa una misma investigación”.

b) Análisis Documental

Este tipo de técnica obtiene datos de fuentes secundarias como son libros, tesis, doctorados, revistas, periódicos entre otros, se utilizan como fuentes para recolectar datos sobre las variables de interés.

CAPITULO IV: DESARROLLO DE LA PROPUESTA DE INVESTIGACION

4.1. TOPOLOGIA DE LA PROPUESTA

Para el desarrollo de esta investigación se propuso utilizar un servidor web que fuera accesible para cualquier persona en el mundo, y careciendo de una IP Publica fija por ser costosa adquirirla, optamos por usar el servicio de DNS gratuito que nos ofrece **No-IP** de esta manera para cualquier usuario estaría disponible nuestro servidor web ya sea con una página web informática o desarrollada para ofrecer distintos tipos de servicios a los usuarios finales.

Teniendo en cuenta que todo tipo de servicio que una empresa ofrece al público en general es vulnerable a distintos tipos de ataques como Fuerza bruta, Inyección SQL, ataques DoS entre otros, entonces se planteó ubicar el servidor web en una DMZ (Zona Desmilitarizada) con el fin de evitar comprometer la red interna ante cualquier ataque informático.

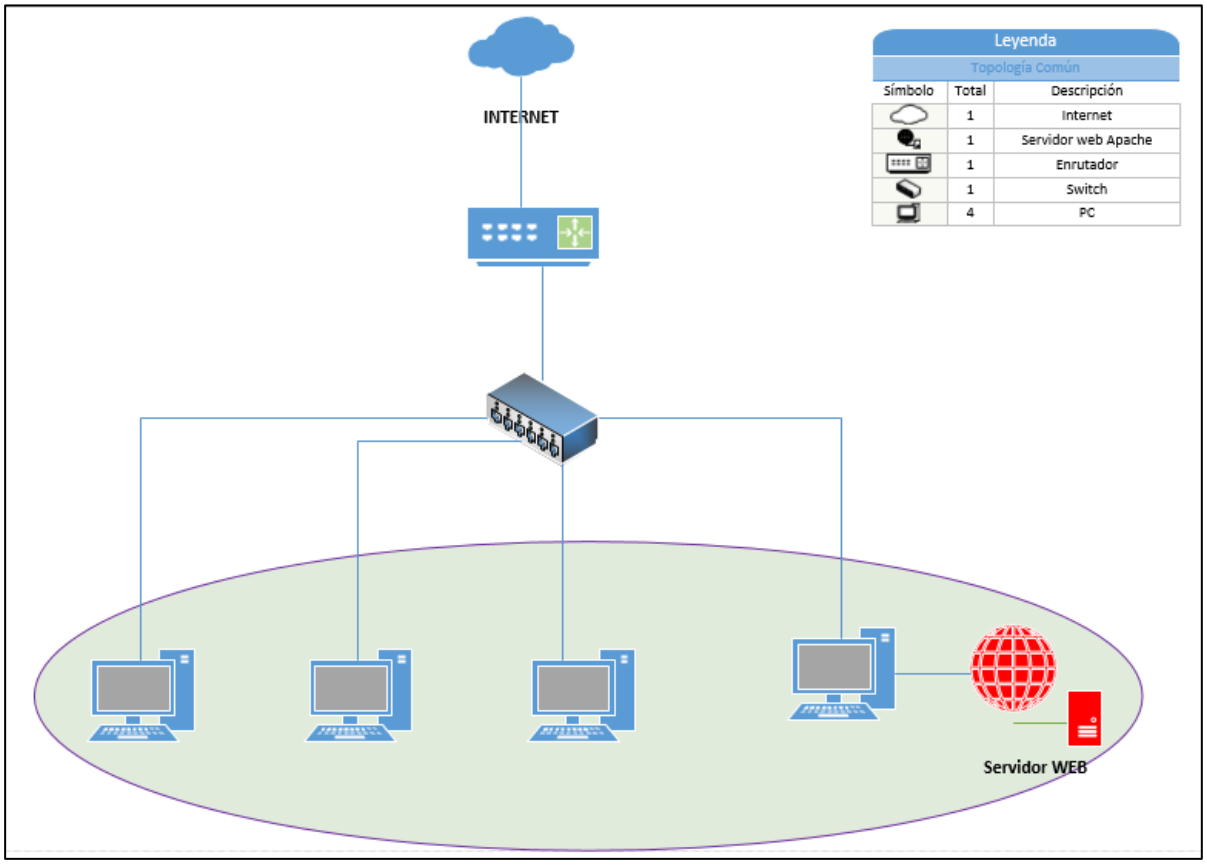


Figura 19 Topología de red local sin propuesta de protección para el servidor web

Fuente: Elaboración Propia

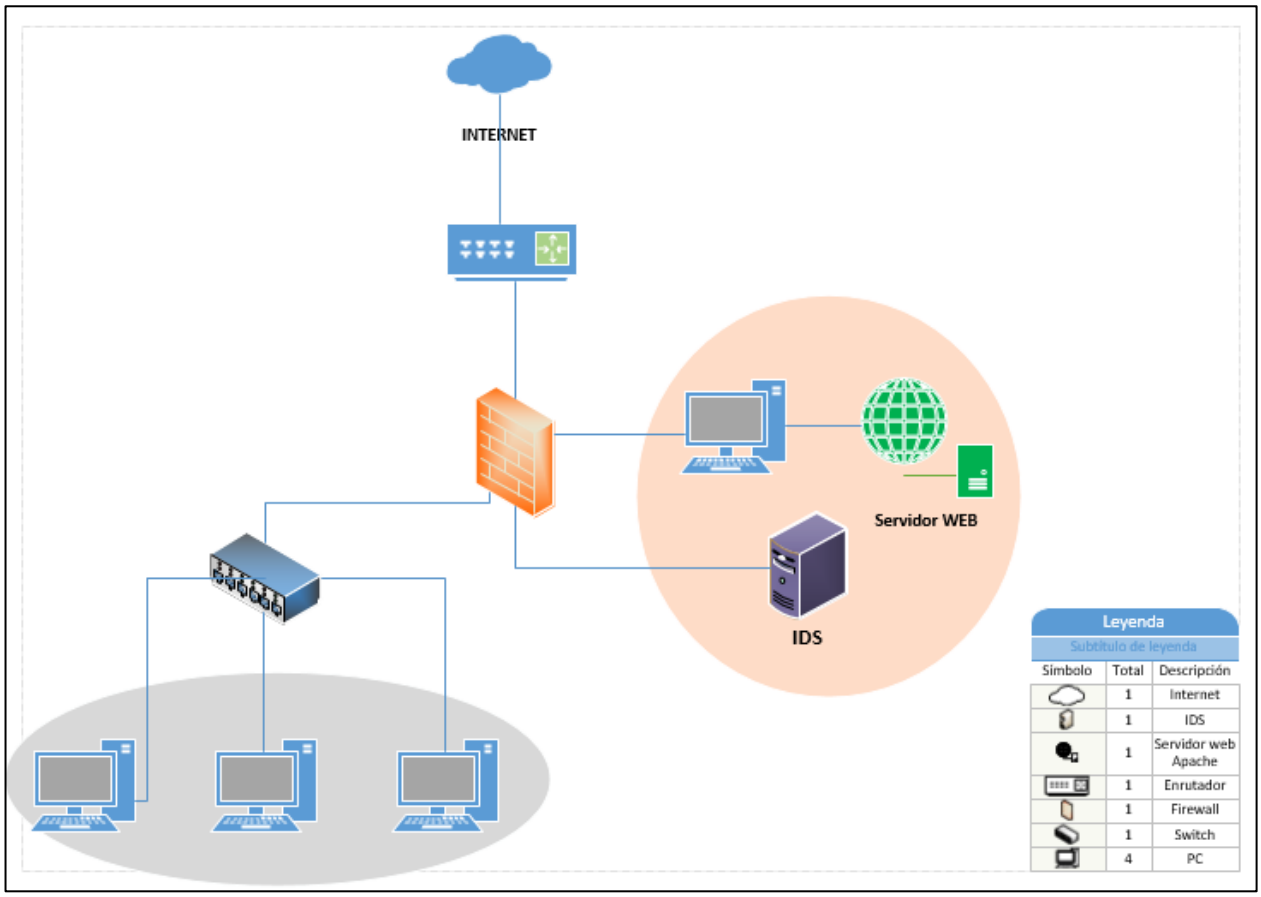


Figura 20 Topología de red propuesta para proteger el servidor web

Fuente: Elaboración Propia

Si tenemos el servidor web dentro de una DMZ protegemos la red interna de los usuarios que trabajan para la empresa reduciendo de cierta manera el impacto de un ataque informático

Para tener una idea de cómo debe ser la red local de un atacante y considerando que sería un usuario normal desde casa o desde cualquier otro lado pero siempre con acceso a internet cualquiera de las siguientes topologías se debería presentar ante un ataque DoS

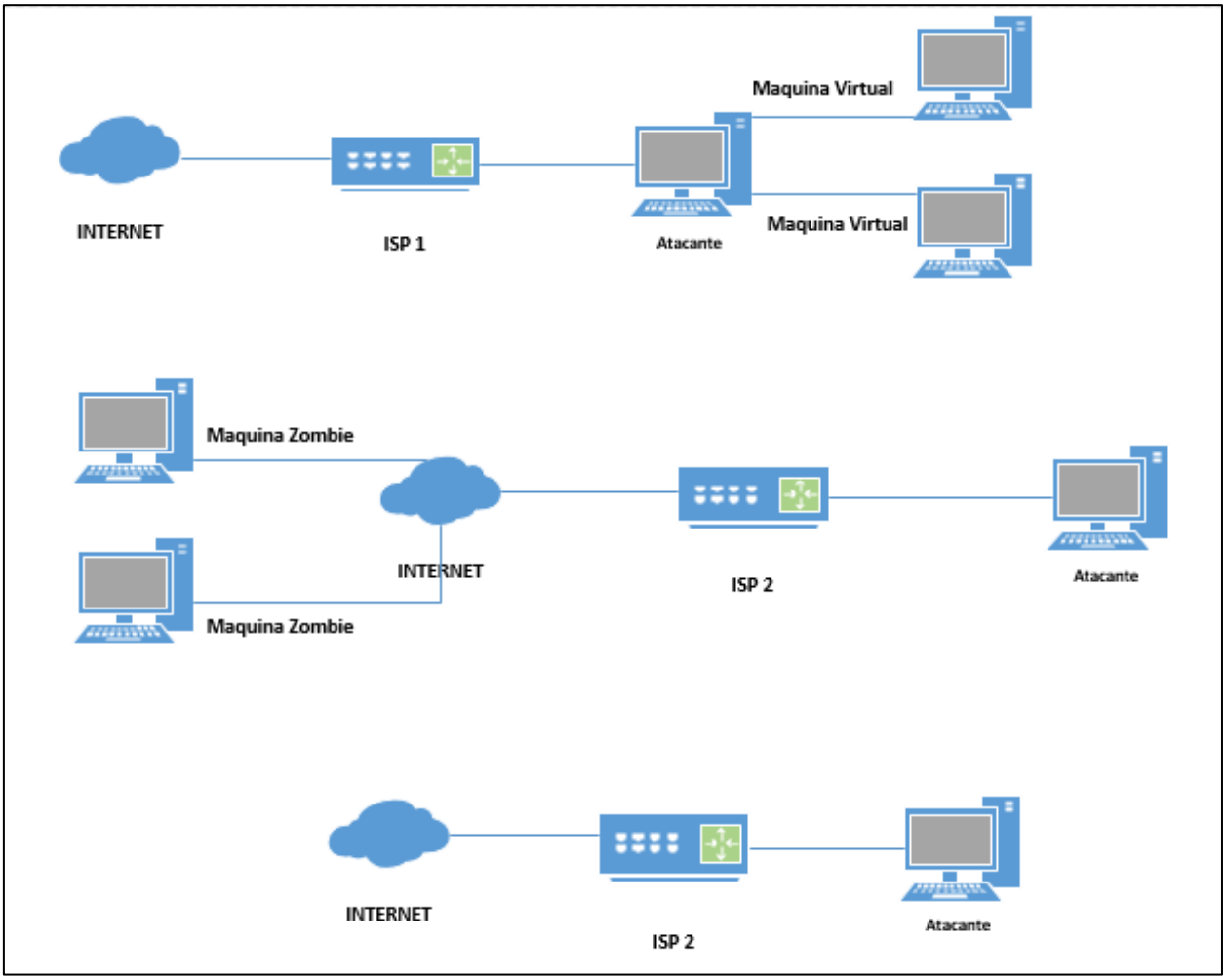


Figura 21 Posibles topologías de la red para un ataque DoS

Fuente: Elaboración Propia

4.2. ASPECTOS TÉCNICOS

Para el desarrollo de esta propuesta utilizamos los siguientes equipos Físicos y Virtuales, para que según sus características cumplan con una tarea específica.

Equipo Fisico	Función	Sistema Operativo Principal	Memoria RAM	Sistema Operativo Virtual	RAM Virtual
RED LOCAL EMPRESA					
PC1	Servidor WEB	Windows 10	8 GB	Ubuntu 16	1 GB
	IDS	Windows 10	8 GB	Ubuntu 16	1 GB
PC2	Usuario Legitimo	Windows 7	2 GB	***	***
RED LOCAL USUARIOS EXTERNOS					
PC3	Usuario Legitimo	Windows 7	4 GB	***	***
PC4	Usuario Legitimo	Windows 10	8 GB	***	***
RED LOCAL USUARIOS ATACANTES					
PC5	Usuario Atacante	Windows 10	8 GB	***	***
PC6	Usuario Atacante	Windows 7	2 GB	***	***

Tabla 4 Aspectos Técnicos

Fuente: Elaboración Propia

4.3. HERRAMIENTAS DE VIRTUALIZACION

Podemos utilizar diferentes herramientas de virtualización, entre las más conocidas encontramos **VMWare** y **VirtualBox,** de las cuales para este desarrollo usaremos **VMWare** la versión gratuita

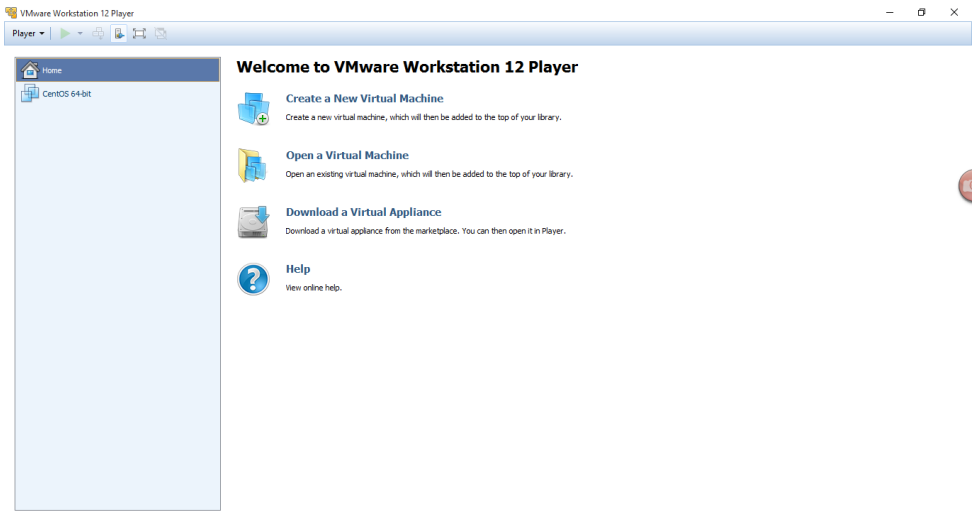


Figura 22 Interface VMWARE Player

Fuente: Elaboración Propia

4.4. INSTALACION DE SERVIDOR WEB APACHE Y PUBLICACION EN INTERNET

1. Teniendo en cuenta que el servidor web estará bajo el entorno de Ubuntu Grafico, con el comando **lsb_release –a** podemos ver la versión.

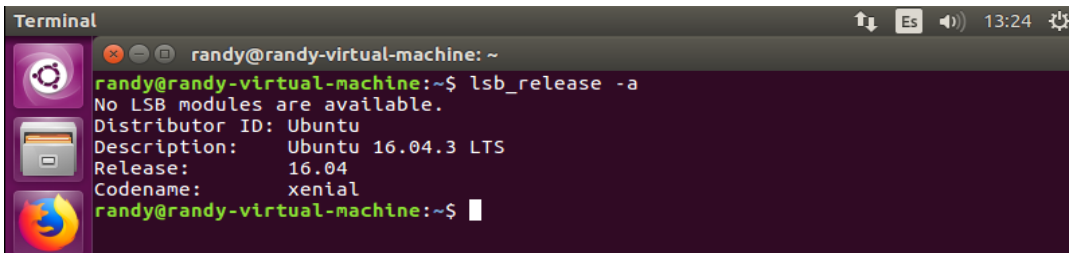


Figura 23 Comandos Versión UBUNTU

Fuente: Elaboración Propia

Antes de instalar apache en el S.O debemos ejecutar un par de comandos en el terminal de Ubuntu

- **sudo apt-get update**
- **sudo apt-get upgrade**

El comando **sudo** hace referencia al **super usuario** el cual tiene todos los permisos para ejecutar comandos en Ubuntu.

Luego de ejecutar esos dos comandos en la misma ventana terminal de Ubuntu ejecutaremos la siguiente línea

- **sudo apt-get install apache2**

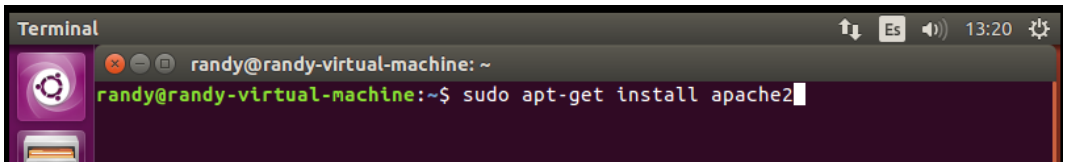


Figura 24 Comandos Install Apache Server

Fuente: Elaboración Propia

Para verificar que apache se instaló podemos utilizar el siguiente comando:

- **apache2ctl -v**

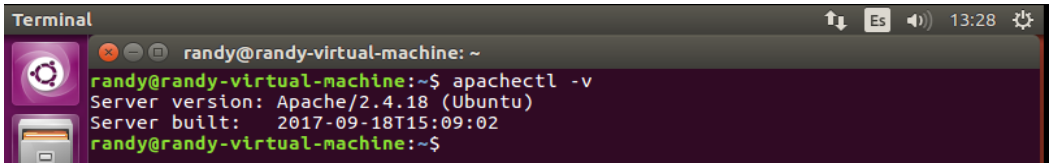


Figura 25 Comandos versión Apache

Fuente: Elaboración Propia

Finalmente, solo queda modificar la página web que sale por defecto al instalar apache.

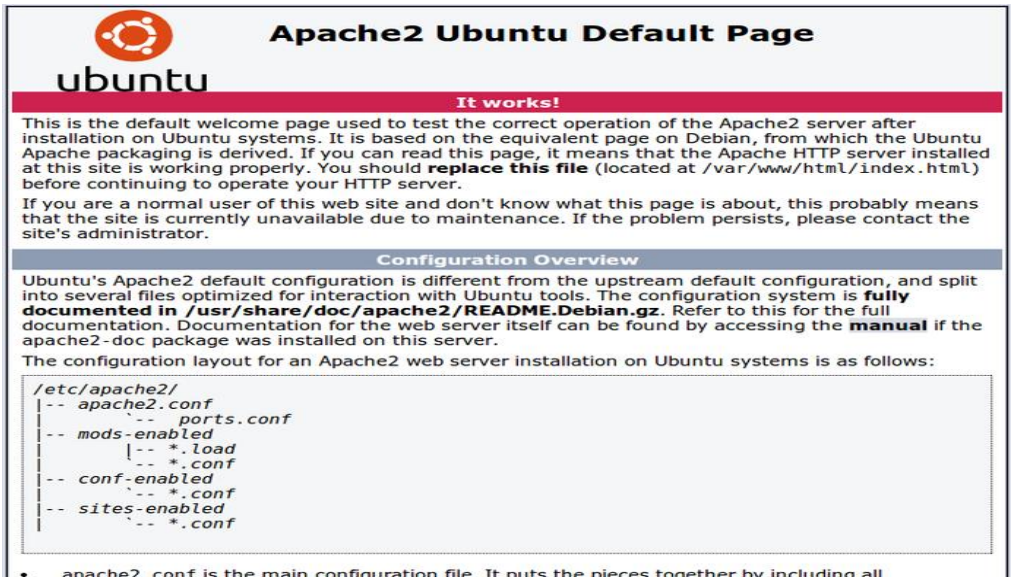


Figura 26 Página WEB por default Apache

Fuente: Elaboración Propia

Utilizaremos la interfaz del negocio de un café cualquiera, quedando de la siguiente manera

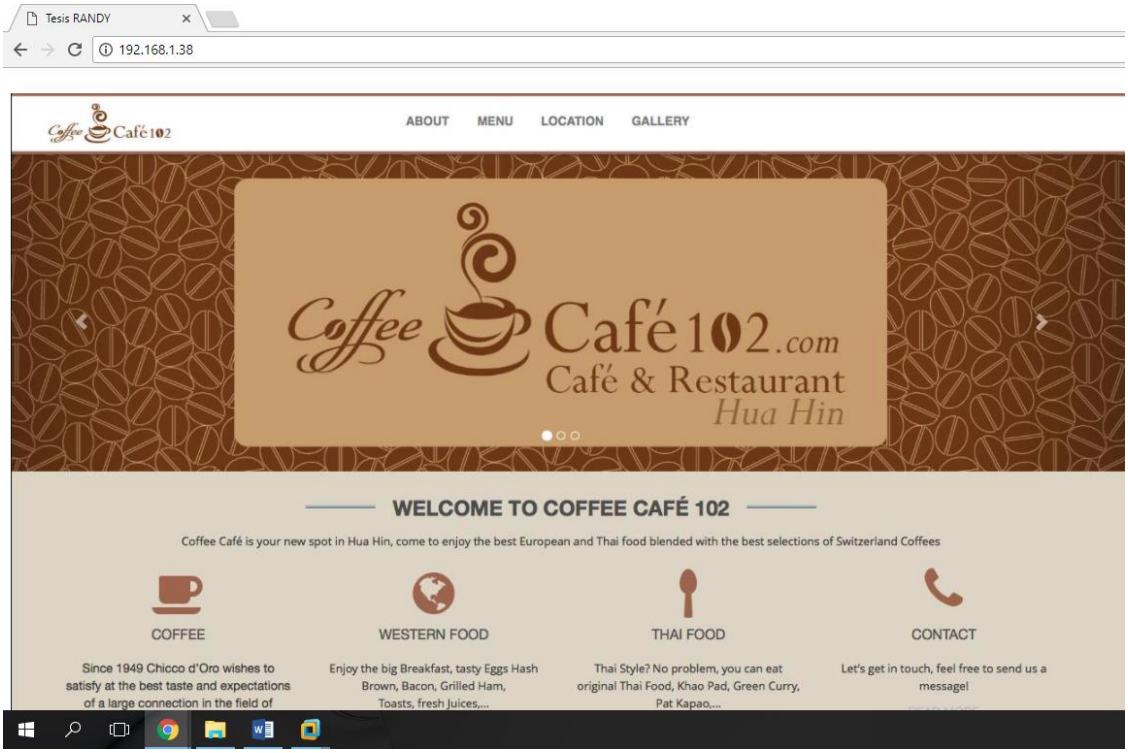


Figura 27 Página WEB Tesis Café

Fuente: Elaboración Propia

Para publicar nuestra web en internet utilizaremos el servicio que ofrece de **NoIP**

¿Qué es NoIP?

NO-IP es en términos muy simples un servicio que se utiliza para asignarle a tu IP un nombre de dominio gratuito

Es un servicio de DNS como varios en el mercado, por ejemplo, OpenDNS y DynDNS, este último sufrió precisamente un ataque DoS en el 2017 afectando a miles de empresas que tenían contratado el servicio DNS con esta empresa

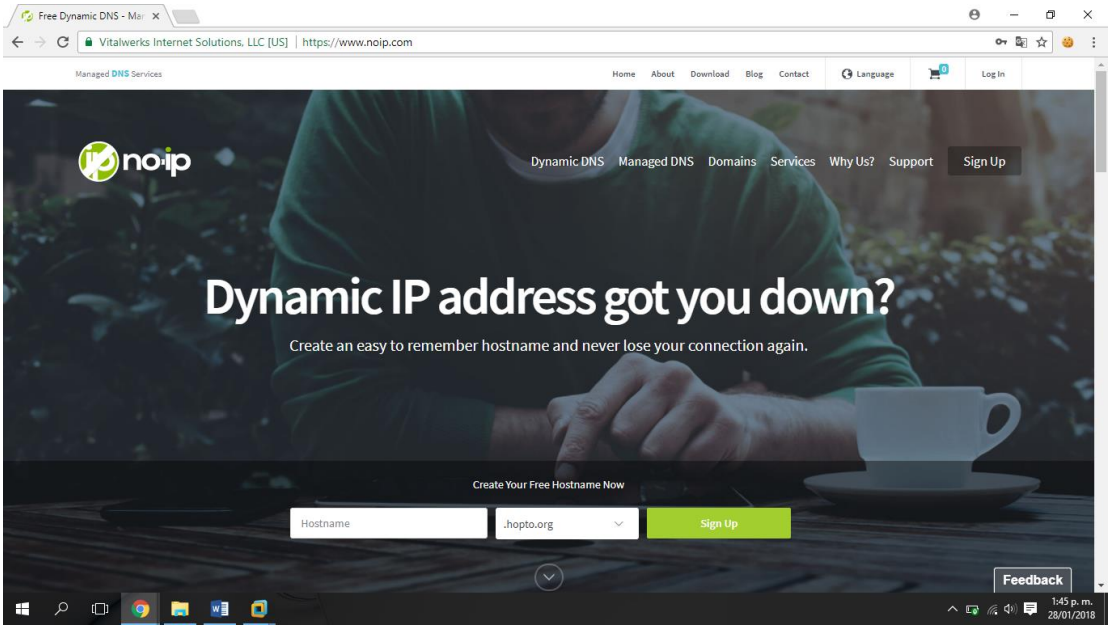


Figura 28 Página Web No-IP

Fuente: https://www.noip.com/

Debemos crearnos una cuenta en la página web de **NoIP** (https://www.noip.com) y registrar un dominio agregando nuestra IP Pública

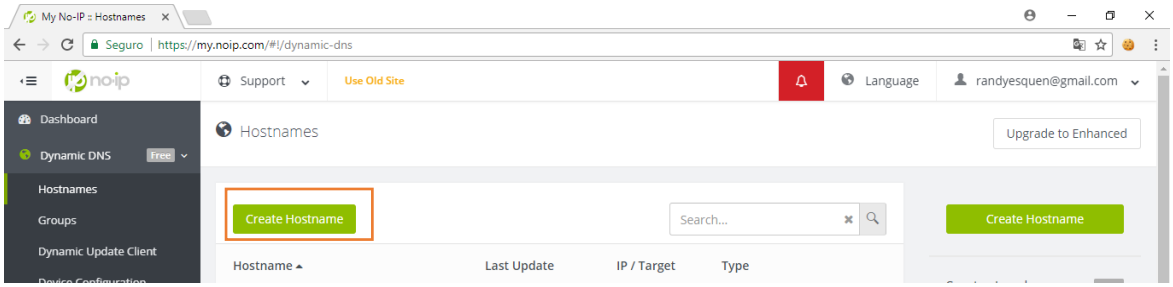


Figura 29 Página Web No-IP – HostName

Fuente: Elaboración Propia

Creamos un Hostname y escribimos nuestra Ip Publica, la cual la encontramos en nuestro router o escribiendo en internet “Cual es mi ip”

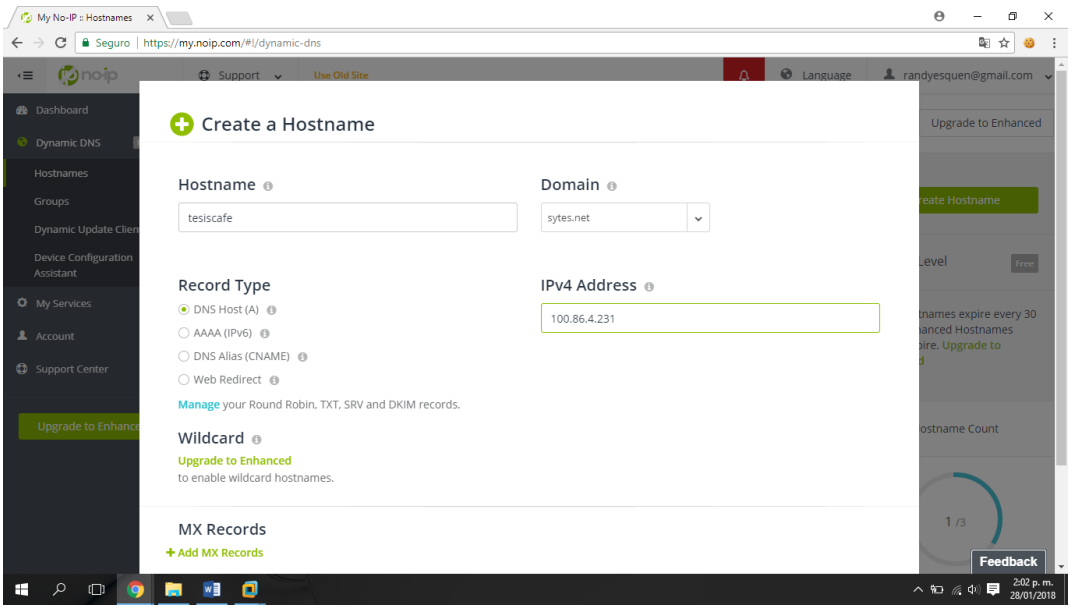


Figura 30 Página Web No-IP – Create HostName

Fuente: Elaboración Propia

Quedando de la siguiente manera

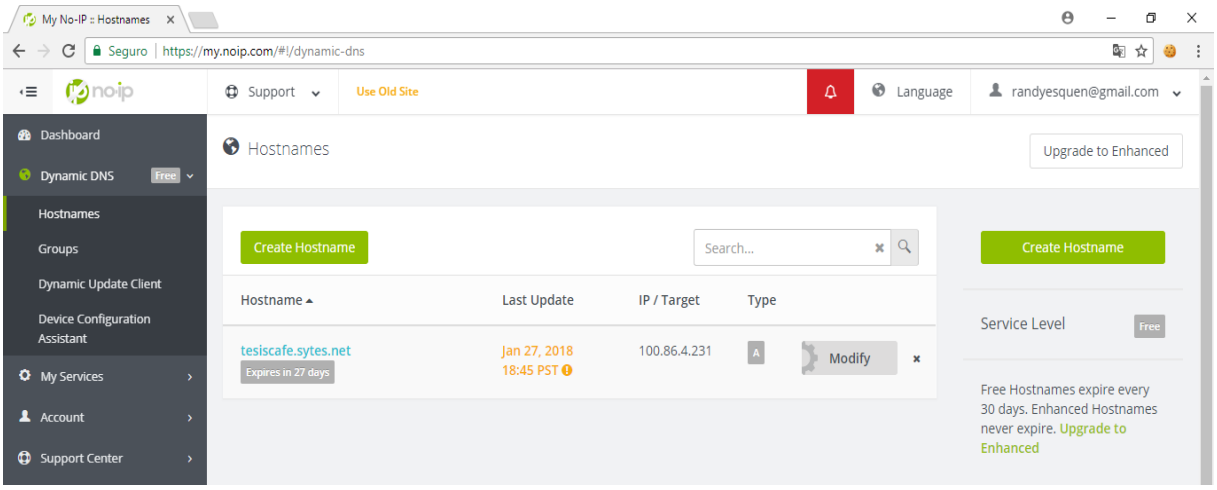


Figura 31 Página Web No-IP – Pizarra HostName

Fuente: Elaboración Propia

Ahora pasamos a ejecutar otros comandos en la ventana terminal de Ubuntu para anexar nuestro terminal con el dominio que creamos en NoIP

Instalar-Noip-Ubuntu: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
INSTALAR NO-IP

        A) Entramos o tecleamos en la terminal este comando para accesar donde pondremos el no-ip
        cd /usr/local/src/

        B) descargamos el programa de No-Ip
        sudo wget http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz

        C) Descomprimimos el fichero
        sudo tar xf noip-duc-linux.tar.gz

        D) Entramos a la carpeta que se nos creo al descomprimir el rar
        cd noip-2.1.9-1/ o buscarlo usr/local/src y copiarlo en "Carpeta Personal"

        E) Y lo instalamos
        sudo make install  (Ingresar login/email y password, colocar 30, y, no-ip)

        F) Para ejecutar el programa, solo tendremos que introducir el siguiente comando.
        sudo /usr/local/bin/noip2
```

Figura 32 Configuración No-IP en Apache

Fuente: Elaboración Propia

Finalmente abrimos un navegador web cualquiera y escribimos el dominio registrado anteriormente en NoIP

Figura 33 Página Web Tesis

Fuente: Elaboración Propia

4.5. MECANISMOS DE ATAQUE DOS

Luego de estudiar los tipos de ataques DoS en el punto **2.2.7** de esta investigación, el tipo de ataque que usaremos es un tipo de ataque basado en volumen, para lo cual usaremos la herramienta HTTP Attack.

- **HTTP ATTACK**

Sobre este tipo de ataque (Britos, 2010) indica lo siguiente:

Este software realiza la función de generar tráfico TCP/IP a través del puerto 80, creando múltiples conexiones al servidor web al mismo tiempo.

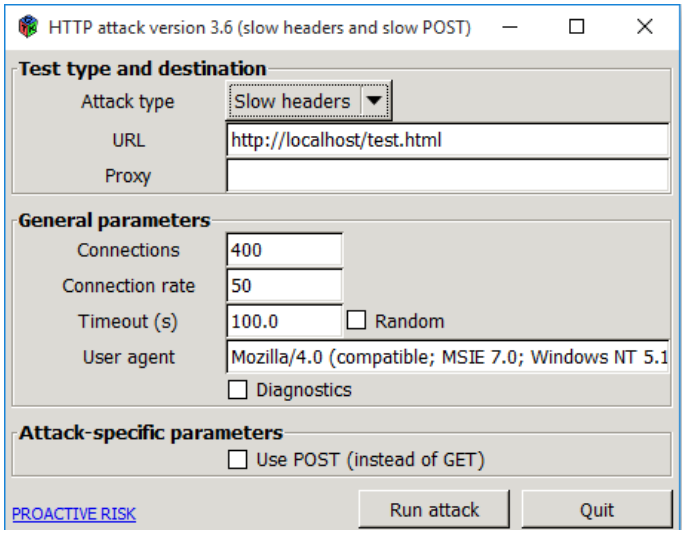


Figura 34 Página Web Tesis

Fuente: Elaboración Propia

4.6. MECANISMOS MONITOREO

Usamos la herramienta **Netstat** en el servidor web para monitorear la cantidad de conexiones existentes, para ello es necesario los siguientes parámetros:

```
[root@leon: ~] netstat -an | grep :80 | sort
```

Figura 35 Herramienta Netstat

Fuente: Elaboración Propia

4.7. MECANISMOS DE SEGURIDAD CONTRA ATAQUES DOS

Después de identificar los mecanismos de protección contra ataques DoS, estudiados los puntos **2.2.11** y **2.2.12**, utilizaremos Snort e IPTables como mecanismos de protección contra ataques DoS.

- **SNORT**

Unos de los mecanismos de seguridad que escogimos para esta propuesta de solución a los ataques DoS es SNORT por ser un sistema de detección de intrusos en red, libre y gratuito.
Se usará como un NIDS que nos permitirá sniffear la red para detectar los ataques DoS además de contar con un modo consola también se implementara un modo grafico para que los usuarios que no tengan muchos conocimientos informáticos puedan ver en una pantalla como están las peticiones hacia el servidor web.

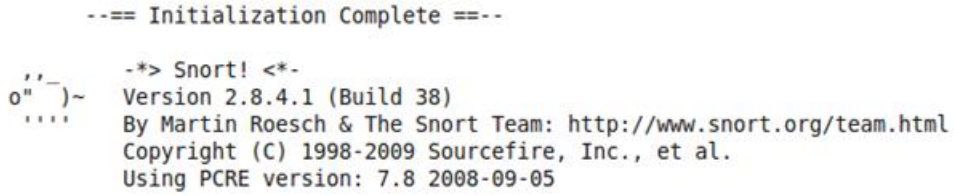


Figura 36 Inicialización Snort

Fuente: Elaboración Propia

- **IPTables**

IPTables es un poderoso firewall integrado en el kernel de Linux y que funciona tanto para IPv4 como para IPv6, (IPTables – IP6Tables)
IPTables ya viene integrado en el sistema, por lo que no es un servicio que se inicia o se detiene, simplemente se configuran reglas y se aplican una serie de políticas de seguridad, como, por ejemplo:

- **ACCEPT:** Acepta la petición.
- **DROP:** Rechaza la petición.
- **REJECT:** Rechaza la petición y notifica al emisor
- **QUEUE:** Introduce el paquete en una cola dentro de la biblioteca.
- **RETURN:** El paquete vuelve a su origen y deja de circular por la cadena.

- **LOG:** Crea un registro de los paquetes que circulan por la cadena.
- **DNAT:** Modifica la dirección de destino (Destination NAT) y su puerto.
- **SNAT:** Modifica la dirección de origen (Source NAT) y su puerto.

4.8. IMPLEMENTAMOS LOS MECANISMOS DE SEGURIDAD QUE MITIGUEN A LOS ATAQUES INFORMATICOS

4.8.1. IMPLEMENTACION DE MECANISMOS APACHE MOD EVASIVE Y MOD SECURITY

Para implementar estos dos módulos de apache se utilizará una máquina virtual la cual tendrá instalado una versión de Ubuntu 16 con entorno grafico amigable al usuario final, La tesis que propone esta solución fue desarrollada por (Britos, 2010), utilizaremos las versiones actuales de dichos mecanismos con las mismas configuraciones por la tesis propuesta anteriormente para saber si siguen siendo efectivos contra los ataques DoS.

Pasos:

1. Primero abrimos una ventana de terminal y ejecutaremos el siguiente comando:
    - **sudo apt-get –y install libapache2-mod-evasive**

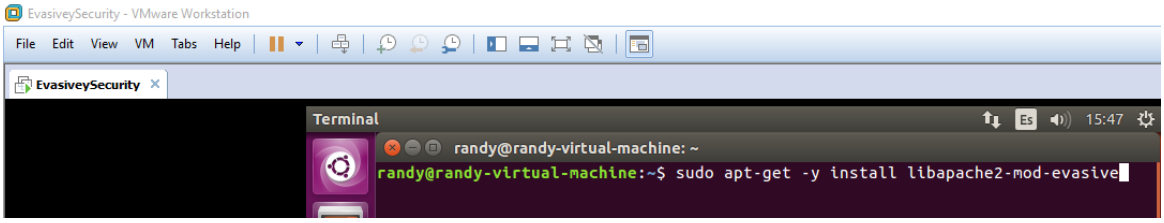


Figura 37 Paso 1 Install Mod_evasive

Fuente: Elaboración Propia

2. Nos dirigimos a la ruta donde se instaló el módulo de apache
    - **cd /etc/apache2/mods-enabled**

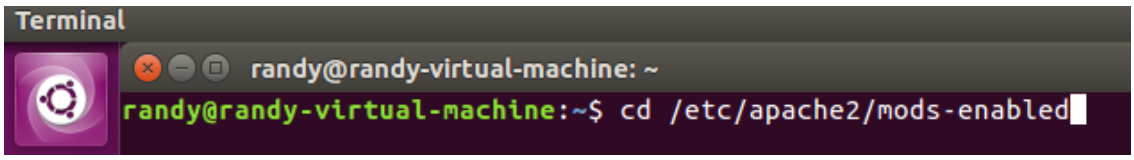


Figura 38 Paso 2 Install Mod_evasive

Fuente: Elaboración Propia

3. Luego editaremos las configuraciones del módulo evasive de apache de la siguiente manera

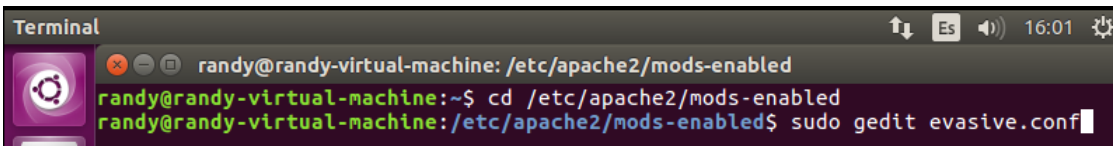


Figura 39 Paso 3 Install Mod_evasive

Fuente: Elaboración Propia

4. Utilizaremos la configuración de la tesis de (Britos, 2010)

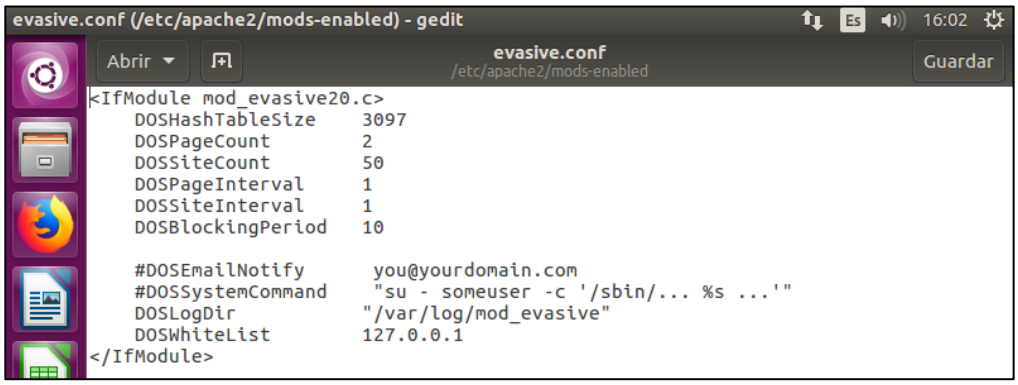


Figura 40 Paso 4 Install Mod_evasive

Fuente: Elaboración Propia

5. Ahora procederemos a la instalación del **mod_security** también de apache, para ello con el siguiente comando

   - **sudo apt-get –y install libapache2-mod-security2**

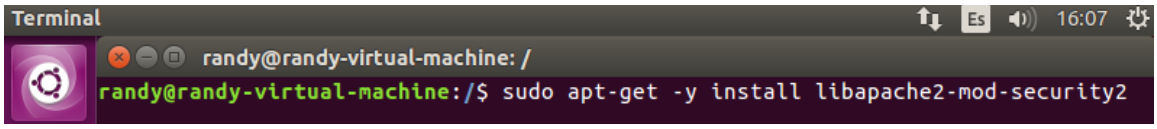


Figura 41 Paso 1 Install Mod_security

Fuente: Elaboración Propia

6. Configuramos tal cual la tesis de (Britos, 2010)

   - **sudo gedit /etc/modsecurity/modsecurity.conf**

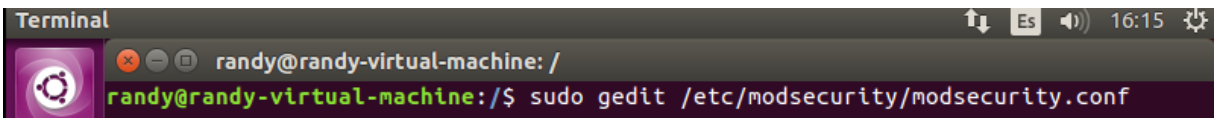


Figura 42 Paso 2 Install Mod_security

Fuente: Elaboración Propia

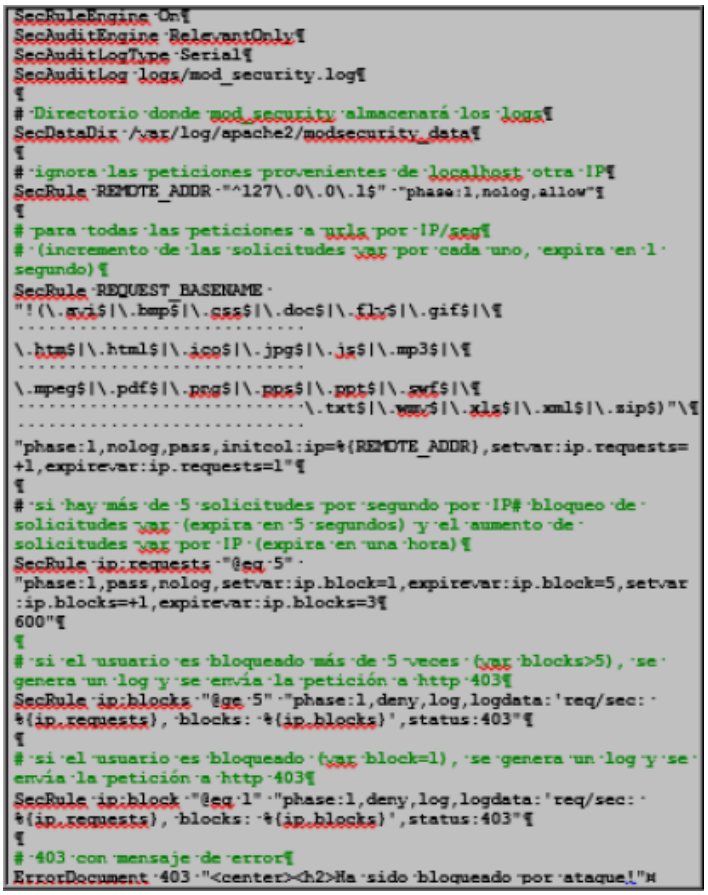


Figura 43 Paso 3 Install Mod_security

Fuente: Tesis (Britos, 2010)

7. Finalmente para activar ambos módulos de apache se ejecutan los siguientes comandos

    - Reiniciamos el servidor para que se activen las reglas de mod_security y seguidamente ejecutamos el comando **sudo a2enmod evasive** para activar el mod_evasive

```
randy@randy-virtual-machine:/$ sudo /etc/init.d/apache2 restart
```

Figura 44 Comando para reiniciar el servicio de apache

Fuente: Elaboración Propia

```
randy@randy-virtual-machine:/$ sudo a2enmod evasive
```

Figura 45 Activación del Mod_evasive

Fuente: Elaboración Propia

4.8.2. IMPLEMENTACION DE MECANISMO SNORT + IPTABLES

A) SNORT IDS

Snort se instalará en un entorno consola de Ubuntu, para ello seguiremos los siguientes pasos:

1. Instalaremos las librerías que funcionan en conjunto con Snort
   - sudo apt-get install –y build-essential
   - sudo apt-get install –y libpcap-dev libpcre3-dev libdumbnet-dev
   - sudo apt-get install –y bison flex

2. Creamos una carpeta donde descargaremos DAQ (Data Acquisition library)
   - mkdir ~/snort_src
   - cd ~/snort_src
   - wget https://snort.org/downloads/snort/daq-2.0.6.tra.gz
   - tar –xvzf daq-2.0.6.tar.gz
   - cd daq-2.0.6
   - ./configure
   - Make
   - Sudo make install

   Luego de ejecutar todos los comandos nos deberá mostrar una pantalla con los siguientes datos:

```
Build AFPacket DAQ module.. : yes
Build Dump DAQ module...... : yes
Build IPFW DAQ module...... : yes
Build IPQ DAQ module....... : no
Build NFQ DAQ module....... : no
Build PCAP DAQ module...... : yes
Build netmap DAQ module.... : no
```

Figura 46 Activación del Mod_evasive 2

Fuente: Elaboración Propia

   - sudo apt-get install –y zlibig-dev liblzma-dev openssl libssl-dev
   - sudo apt-get install –y libnghttp2-dev
   - sudo apt-get install –y autoconf libtool pkg-config
   - cd ~/snort_src

- wget https://github.com/nghttp2/nghttp2/releases/download/v1.17.0/nghttp2-1.17.0.tar.gz
- tar –xzvf nghttp2-1.17.0.tar.gz
- cd nghttp2-1.17.0
- autoreconf –i - -force
- automake
- autoconf
- ./configure - -enable-lib-only
- make
- sudo make install

3. Instalación de Snort
   - cd ~/snort_src
   - wget https://snort.org/downloads/snort/snort-2.9.9.0.tar.gz
   - tar –xvzf snort-2.9.9.0.tar.gz
   - cd snort-2.9.9.0
   - ./configure - -enable-sourcefire
   - make
   - sudo make install
   - sudo ldconfig

   - snort –v (Para verificar la versión de snort instalada)

-

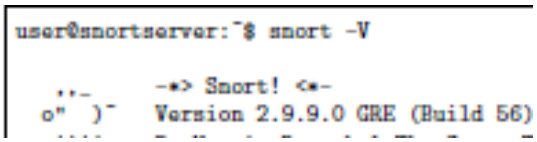


Figura 47 Verificar versión de Snort

Fuente: Elaboración Propia

4. Configuraciones de snort como IDS
   - Creamos usuario y grupos:
     - sudo groupadd snort
     - sudo useradd snort –r –s /sbin/nologin –c SNORT_IDS –g snort
   - Creamos los directorios para Snort
     - sudo mkdir /etc/snort

- sudo mkdir /etc/snort/rules
- sudo mkdir /etc/snort/rules/iplist
- sudo mkdir /etc/snort/preproc_rules
- sudo mkdir /usr/local/lib/snort_dynamicrules
- sudo mkdir /etc/snort/so_rules

- Creamos algunos archivos para guardar reglas y listas ip
  - sudo touch /etc/snort/rules/iplist/black_list.rules
  - sudo touch /etc/snort/rules/iplist/white_list.rules
  - sudo touch /etc/snort/rules/local.rules
  - sudo touch /etc/snort/sid-msg.map

- Creamos nuestros directorios de logs
  - sudo mkdir /var/log/snort
  - sudo mkdir /var/log/snort/archived_logs

- Brindamos permisos a las carpetas
  - sudo chmod –R 5775 /etc/snort
  - sudo chmod –R 5775 /var/log/snort
  - sudo chmod –R 5775 /var/log/snort/archived_logs
  - sudo chmod –R 5775 /etc/snort/so_rules
  - sudo chmod –R 5775 /usr/local/lib/snort_dynamicrules
  - sudo chown –R snort:snort /etc/snort
  - sudo chown –R snort:snort /var/log/snort
  - sudo chown –R snort:snort /usr/local/lib/snort_dynamicrules
- Snort necesita algunos archivos de configuración y los preprocesadores dinámicos copiados del paquete de fuente de Snort en la carpeta /etc/snort.

  - cd ~/snort_src/snort-2.9.9.0/etc/
  - sudo cp *.conf /etc/snort
  - sudo cp *.map /etc/snort
  - sudo cp *.dtd /etc/snort
  - cd ~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/buid/usr/local/lib/snort_dynamicpreprocessor/
  - sudo cp * /usr/local/lib/snort_dynamicpreprocessor/

- Necesitamos editar el archivo de configuración principal de snort (/etc/snort/snort.conf), pero antes de eso con

este comando comentaremos algunas líneas por defecto del archivo snort.conf

- sudo sed –i “s/include \$RULE_PATH\#include \$RULE _PATH/” /etc/snort/snort.conf

- Procedemos a editar el archivo snort.conf

  - sudo vi /etc/snort/snort.conf
    - ipvar HOME_NET 192.168.1.0/24
    - ipvar EXTERNAL_NET any

  - Modificamos las rutas de los archivos que contienen las reglas para snort

    - var RULE_PATH /etc/snort/rules
    - var SO_RULE_PATH /etc/snort/so_rules
    - var PREPROC_RULE_PATH /etc/snort/preproc_rules
    - var WHITE_LIST_PATH /etc/snort/rules/iplist
    - var BLACK_LIST_PATH /etc/snort/rules/iplist
    - include $RULE_PATH/local.rules

- Para validar que la configuración de snort no tiene errores escribimos el siguiente comando:

  - sudo snort –T –i ens39 –c /etc/snort/snort.conf

```
user@snortserver:~$ sudo snort -T -i eth0 -c /etc/snort/snort.conf
    (...)
    Snort successfully validated the configuration!
    Snort exiting
user@snortserver:~$
```

Figura 48 Comando Snort

Fuente: Elaboración Propia

5. Escribimos algunas reglas para detectar intrusos y peticiones ICMP

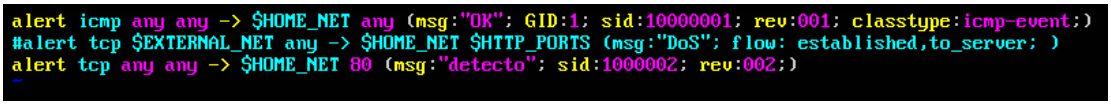


Figura 49 Reglas Snort

Fuente: Elaboración Propia

6. Para mostrar en modo consola lo que capturen las reglas anteriores escribimos el siguiente comando

Figura 50 Comando para monitorear las conexiones que tiene mi servidor web

Fuente: Elaboración Propia

B) IPTABLES

Utilizaremos principalmente una regla que limita la cantidad de conexiones por IP

- **sudo iptables –I INPUT –p tcp - -dport 80 –m connlimit - - connlimit-above 50 - -connlimit-mask 20 –j DROP**

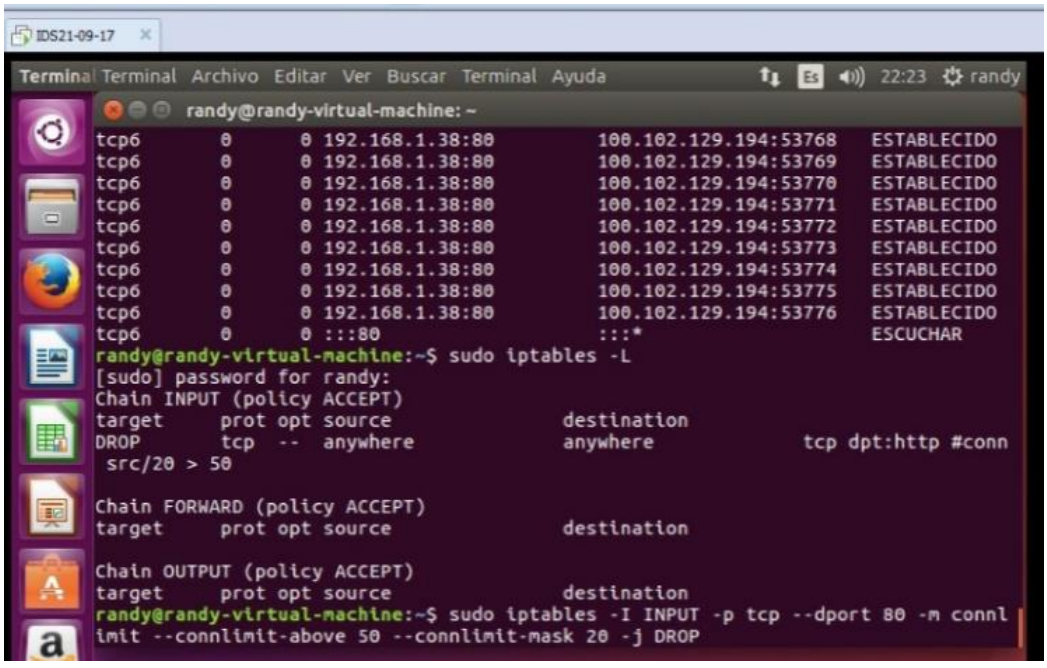


Figura 51 Comando IPTables

Fuente: Elaboración Propia

CAPITULO V: RESULTADOS

5.1. EJECUCION DE ATAQUES AL SERVIDOR WEB

Se realizaron ataques a servidor web con configuraciones distintas:

- **Sin Mecanismos de Seguridad**
- **Mod_Evasive y Mod_Security**
- **Snort + IPTables**

Según nuestra población y muestra calculada en los puntos 3.2 de esta investigación se hicieron pruebas de 40000 peticiones al servidor web por ataque, se usó este número porque es la máxima cantidad de peticiones que puede realizar el HTTP ATTACK y lógicamente en un ataque DoS mientras más fuerte sea este, mejores resultados tendrán para el atacante

La URL que se utilizara para poder acceder a la WEB es http://tesiscafe.sytes.net

5.1.1. SIN MECANISMO DE SEGURIDAD

Se implementó el servidor web sin protección alguna para los ataques DoS con el fin de comprobar si el uso de la herramienta HTTP ATTACK en realidad puede denegar el servicio a un servidor web.

Para ello se levantó el servidor que debería mostrar lo siguiente para cualquier usuario que acceda mediante un navegador ingresando la URL

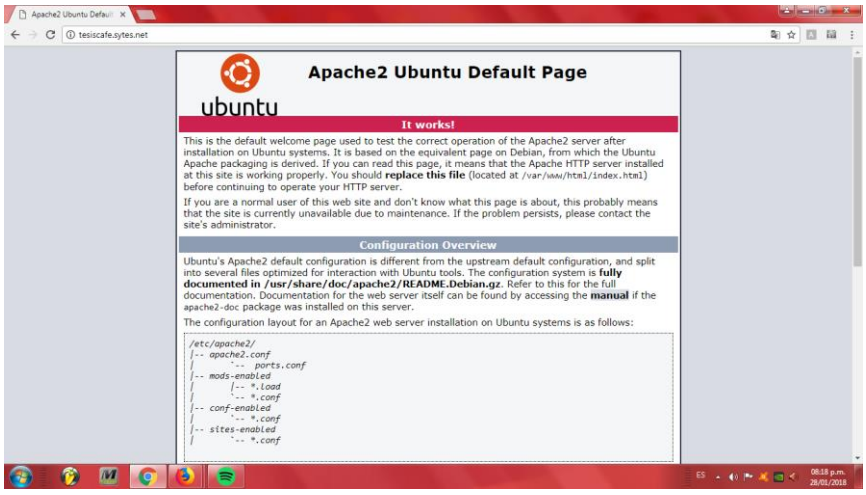


Figura 52 Web sin seguridad

Fuente: Elaboración Propia

Pero luego cuando inicio el ataque con HTTP ATTACK el resultado fue el siguiente

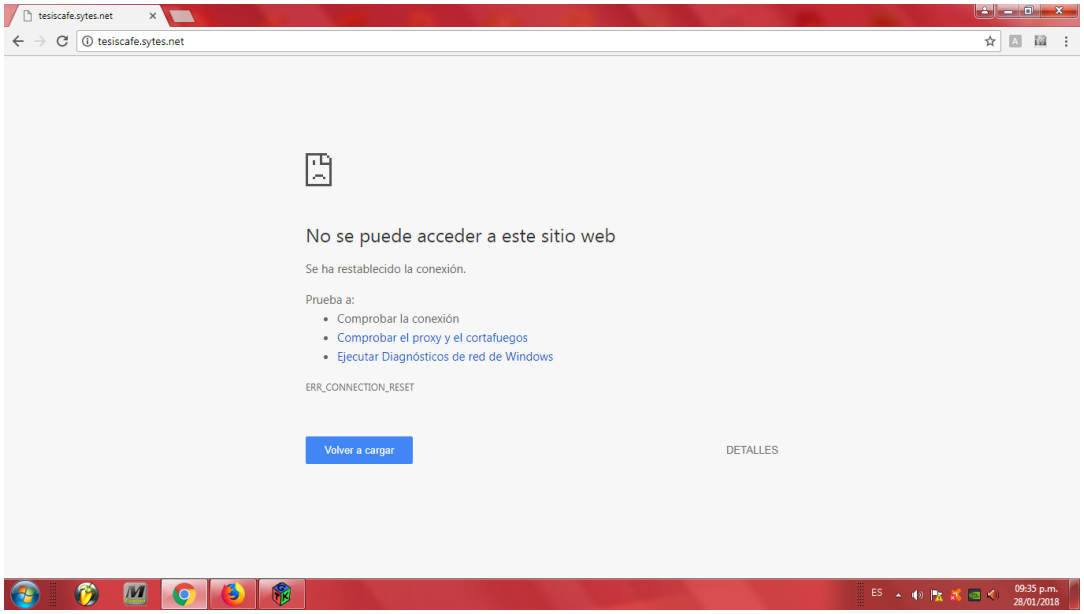


Figura 53 Web sin acceso – Denegado el Servicio

Fuente: Elaboración Propia

5.1.2. MECANISMO DE SEGURIDAD MOD_EVASIVE Y MOD_SECUTIRY (Propuesto por Tesis - Diario Quintana ROO)

Se hicieron las configuraciones respectivas según la tesis de (Britos, 2010) y se cambió el contenido de la página web para poder diferenciar el tipo de configuraciones que se hizo en el servidor, como se muestra en la imagen a continuación

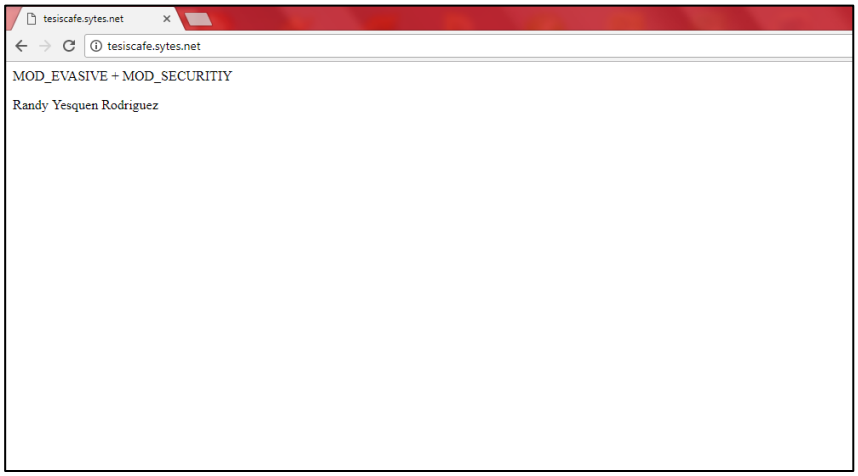


Figura 54 Web con Mod_evasive – Mod_security

Fuente: Elaboración Propia

Luego se procedió a realizar el ataque nuevamente al servidor y el resultado fue que de cada 10 intentos de petición legitimas realizadas por otro usuario solo conectaba 1 o 2 luego de que la página web permaneciera cargando y cargando durante más de 10 min, por lo que en más del 80% de peticiones legitimas al servidor web el resultado fue el siguiente:

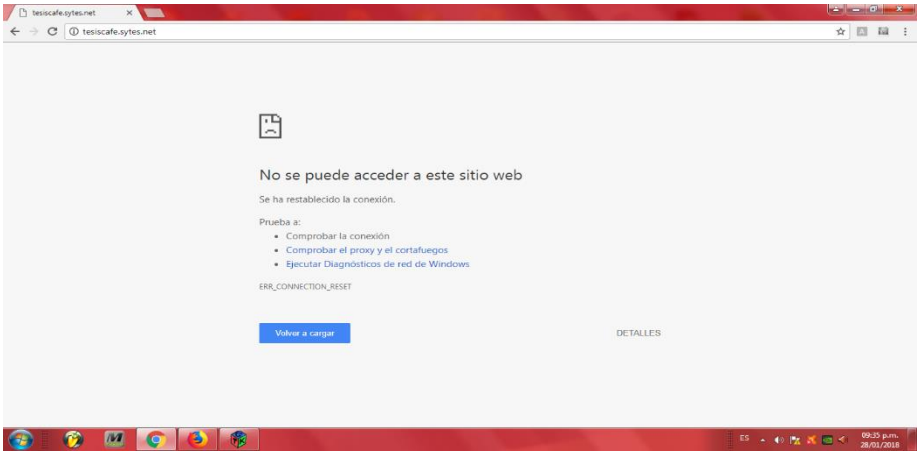


Figura 55 Web – Denegado el Servicio

Fuente: Elaboración Propia

5.1.3. MECANISMO DE SEGURIDAD SNORT E IPTABLES

Para estas pruebas se configuro Snort como IDS e IPTables para mitigar los ataques, seguimos usando la misma URL, luego se puso disponible para cualquier usuario la siguiente web:

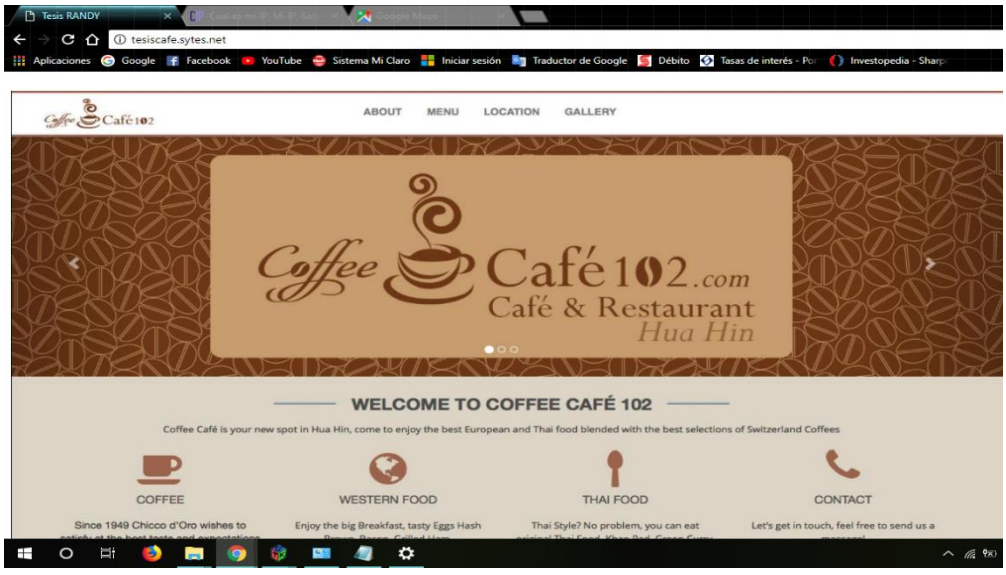


Figura 56 Web con IPTables

Fuente: Elaboración Propia

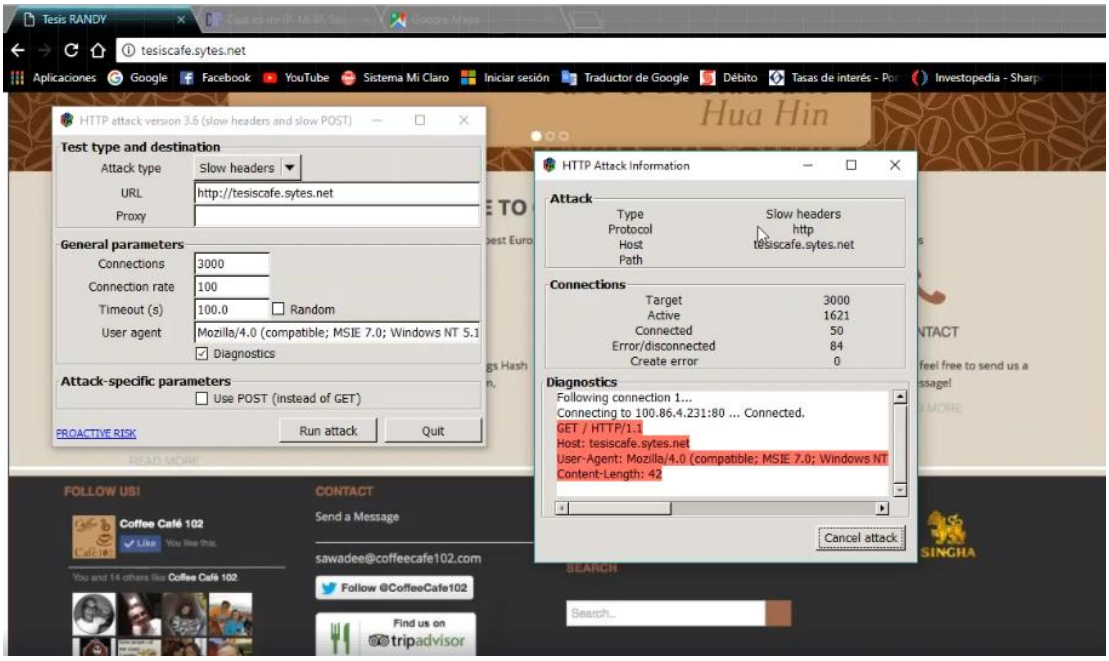


Figura 57 Página bajo ataque HTTP - Attack

Fuente: Elaboración Propia

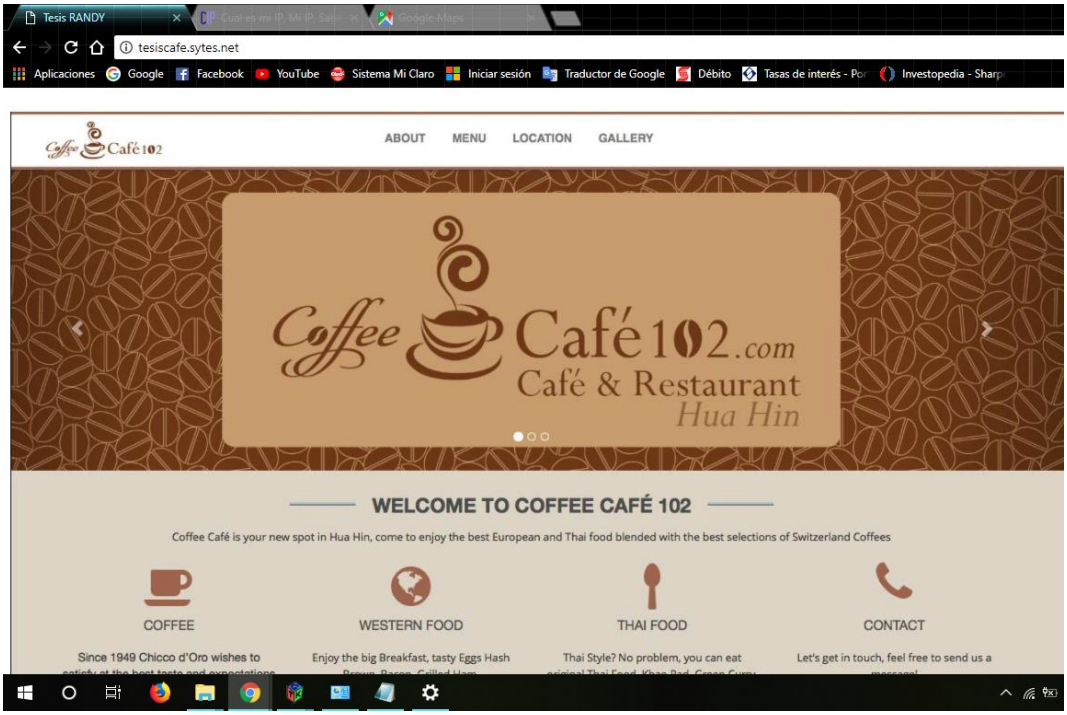


Figura 58 Página disponible después del ataque

Fuente: Elaboración Propia

5.2. COMPARACION DE LOS MECANISMOS DE SEGURIDAD

5.2.1. RESULTADOS DE LOS MECANISMOS CON SUS RESPECTIVOS INDICADORES

Luego de realizar todas las pruebas necesarias pudimos recopilar datos que nos servirán para hacer la comparación de los mecanismos Anti-DoS y así poder determinar cuál es el más efectivo.

a) Servidor Web configuración por defecto

- **Verdaderos Positivos**
  - Ataques correctamente Detectados
- **Verdaderos Negativos**
  - Trafico Normal no detectado como ataque
- **Falsos Positivos**
  - Trafico normal detectado como ataque
- **Falsos Negativos**
  - Ataque no detectado

Promedio % Disponibilidad = 0 %			
Verdaderos Positivos	**Verdaderos Negativos**	**Falsos Positivos**	**Falsos Negativos**
0 %	0 %	100 %	0 %

Tabla 5

Resultados Web Default
Fuente: Elaboración Propia

Los datos mostrados en la gráfica indican que si no tenemos alguna configuración en el servidor web este permitirá todo tipo de petición al servidor web sea o no legitima lo que hace completamente vulnerable a un ataque DoS

Figura 59 Grafico de Barras – Servidor Web Default

Fuente: Elaboración Propia

b) Servidor Web – Mod_evasive – Mod_security

- **Verdaderos Positivos**
  - Ataques correctamente Detectados
- **Verdaderos Negativos**
  - Trafico Normal no detectado como ataque
- **Falsos Positivos**
  - Trafico normal detectado como ataque
- **Falsos Negativos**
  - Ataque no detectado

Promedio % Disponibilidad = 4.6 %			
Verdaderos Positivos	**Verdaderos Negativos**	**Falsos Positivos**	**Falsos Negativos**
99.3414 %	4.6 %	95.4 %	0.6586 %

Tabla 6 Resultados Mod_evasive – Mod_security

Fuente: Elaboración Propia

Los datos mostrados en la gráfica indican que durante la realización de los ataques DoS el porcentaje que ataques que fueron correctamente detectados fue del 99.34% y los ataques no detectados fueron del 0.65%, pero por otro lado el porcentaje de peticiones legítimas es de 4.6% y las peticiones que fueron detectadas incorrectamente como ataque es del 95.4%

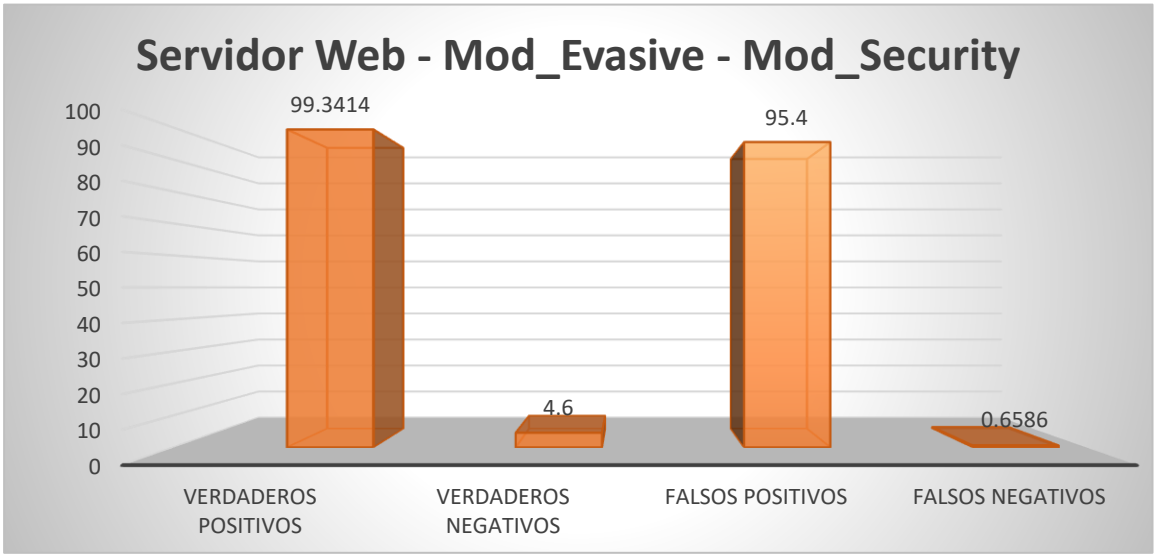


Figura 60 Grafico de Barras – Servidor Web Evasive-Security

Fuente: Elaboración Propia

c) Servidor Web – Snort – IPTables

- **Verdaderos Positivos**
  - Ataques correctamente Detectados
- **Verdaderos Negativos**
  - Trafico Normal no detectado como ataque
- **Falsos Positivos**
  - Trafico normal detectado como ataque
- **Falsos Negativos**
  - Ataque no detectado

Promedio % Disponibilidad = 97.15 %			
Verdaderos Positivos	**Verdaderos Negativos**	**Falsos Positivos**	**Falsos Negativos**
99.8659125 %	97.15 %	2.85 %	0.1340875 %

Tabla 7 Resultados Snort + IPTABLES

Fuente: Elaboración Propia

Los datos mostrados en la gráfica indican que durante la realización de los ataques DoS el porcentaje que ataques que fueron correctamente detectados fue del 99.86% y los ataques no detectados fueron del 0.13%, pero por otro lado el porcentaje de peticiones legítimas es de 97.15% y las peticiones que fueron detectadas incorrectamente como ataque es del 2.85%

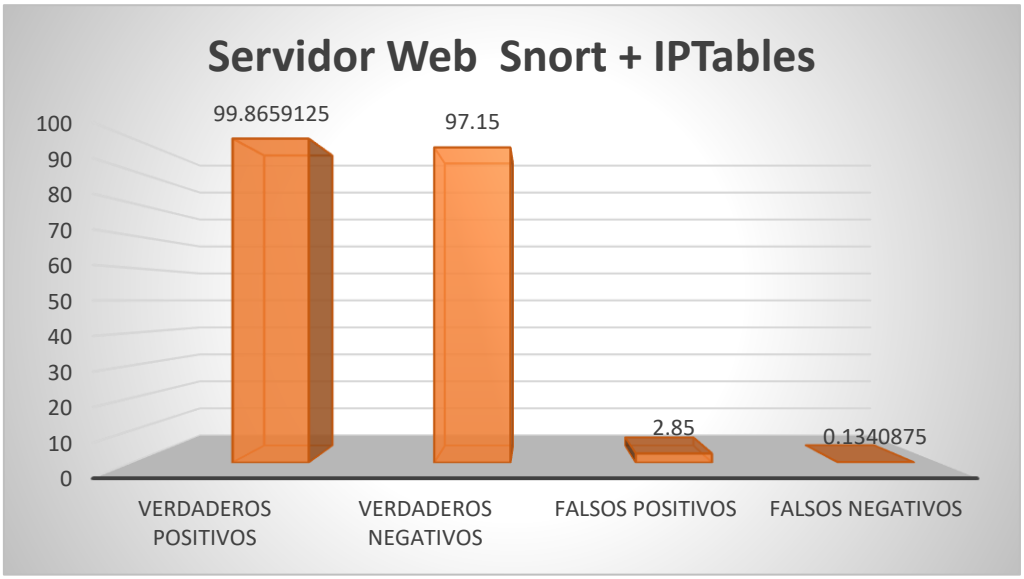


Figura 61 Grafico de Barras – Servidor Web Snort + IPTables

Fuente: Elaboración Propia

5.2.2. ANALISIS DE RESULTADOS

a. Servidor web configuración por defecto

Durante las pruebas realizadas según este modelo se obtuvo que el servidor queda fuera de servicio luego de recibir el ataque DoS. Este modelo permite cualquier tipo de conexión sin ningún control haciendo que el servidor se congestione y el atacante logre su objetivo.

b. Servidor web Mod_evasive – Mod_security

En este modelo propuesto se tiene una mejoría con respecto a los ataques detectados, pero tiene una gran desventaja con las peticiones legítimas, obteniendo un índice de más del 95.4% de peticiones a las cuales no se les permitió el acceso y por el contrario solo un 4.6% de peticiones atendidas.

Se puede deducir que para en este modelo el atacante cumple su objetivo dejando sin servicio al 95.4% aproximadamente de peticiones entrantes que debieron ser atendidas por el servidor.

c. Servidor web – Snort + IPTables

Esta propuesta mejora considerablemente la cantidad de ataques detectados, la cantidad de peticiones legitimas atendidas y reduce la cantidad de peticiones legítimas no atendidas por el servidor.
Durante la realización de estas pruebas el servidor web detecta un 99.86% de ataques, y a diferencia del modelo anterior el servidor web atiende a un 97.15% de las peticiones legitimas realizadas por usuarios del día a día.

Con este modelo el atacante solo logrará dejar sin acceso al 2.85% de usuarios que quieran acceder a la web, lo cual es un buen indicador respecto a los otros dos modelos analizados.

Esta última propuesta cumple con el objetivo de esta investigación, detectando un ataque DoS para posteriormente mitigarlo, manteniendo la disponibilidad del servicio para los usuarios legítimos.

En este ultima figura, luego de analizar los resultados obtenidos en el punto 5.2 de esta investigación podemos observar mediante un gráfico de barras, que el modelo propuesto Snort + IPTables, mantiene mejor la disponibilidad del servidor que los otros dos modelos estudiados.

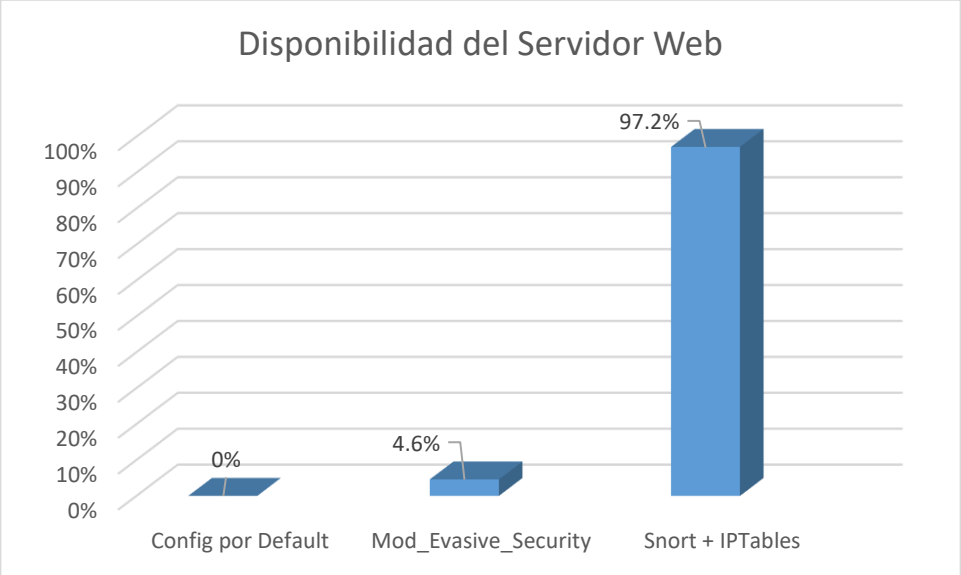


Figura 62 Comparación de Disponibilidad del Servidor

Fuente: Elaboración Propia

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

Después de todas las pruebas realizadas en el desarrollo de esta investigación se llegó a las siguientes conclusiones

- Los tipos de ataques DoS para servidores Web pueden ser ataques basados en Volumen, basados en Protocolos o basados en la capa de Aplicación, siendo los de tipo Volumen los más utilizados por los atacantes por ser difíciles de detectar y fáciles de ejecutar.

- Para el tipo de ataque DoS basados en volumen el mecanismo de protección Snort + IPTables responde de una manera efectiva, protegiendo y manteniendo disponible el servicio web sin que el usuario sienta en algún momento que el servidor está bajo ataque DoS

- Luego de analizar las herramientas Anti-DoS podemos concluir que Snort + IPTables muestra mejores resultados en relación a los módulos de apache, por tener menos tasa de falsos positivos y más tasa porcentual de verdaderos negativos, manteniendo el servicio disponible ante peticiones de usuarios legítimos.

- Se logró demostrar satisfactoriamente que la propuesta de esta investigación puede detectar y mitigar un ataque DoS obteniendo indicadores positivos bastante altos con respecto a las variables de esta investigación, uno de ellos la disponibilidad del servicio web.

6.2. RECOMENDACIONES

- Se recomienda a las micro y pequeñas empresas implementar la solución propuesta al fin de proteger sus servidores web contra ataques DoS, teniendo cuidado al realizar la definición de las múltiples reglas que nos ofrece IPTables y Snort, para así asegurar la disponibilidad del servicio web.

- Las futuras investigaciones interesadas en esta tesis pueden explotar las distintas características de Snort como un IPS, con el fin de mejorar el rendimiento del modelo propuesto.

- Se sugiere investigar más a profundidad las reglas IPTables para protegernos contra otros tipos de ataques informáticos, con el fin de mejorar no solo la disponibilidad si no también la seguridad de nuestro servicio web.

- Se sugiere a las empresas realizar un estudio de la cantidad de peticiones web que recibe por día, mes y año, con el fin de poder tener un intervalo de la cantidad de tráfico web que esta genera, siendo así más fácil reconocer cuando se está bajo un ataque DoS.

REFERENCIAS BIBLIOGRAFICAS

Blacker, W. (2007). *Ataques de denegación de servicio distribuido. Técnicas de Defensa.*

Britos, J. D. (2010). *Detección de intrusiones en redes de datos con captura distribuida y procesamiento estadístico.* Tesis de Maestría.

Campo Giralte, L. (s.f.). *Una arquitectura distribuida para la detección, comunicación y mitigación de la denegación de servicio.* Tesis Doctoral, Universidad Rey Juan Carlos|.

Diaz, V. (2008). *Estudio tecnológico sobre sistemas de detección de intrusos.* Universidad Carlos III de Madrid, España.

Guerrero, S. (s.f.). *Sistema de alertas para la detección de un ataque DDoS.* Universidad Autónoma de Bucaramanga.

Hoyos Llanos, M. S. (2015). *Prototipo de detección de ataques DDoS a partir de máquinas de aprendizaje.* Tesis de Maestría, Universidad Autónoma de Manizales, Manizales, Colombia.

Luna Dominguez, J. E. (2016). *Sistema detector de intrusiones ocupando una red neuronal artificial.* Tesis de Maestría, Universidad Autónoma del Estado de México, México.

W3C. HTTP - Hipertexto Transfer Protocol. Obtenido de https://www.w3.org/Protocols/.

Snort: https://www.snort.org/documents

Netcraft: https://news.netcraft.com/

Suricata: https://suricata-ids.org/features/

https://www.voztovoice.org/sites/default/files/snort_manual.pdf

Maciá Fernández, G. (2007). *Ataques de denegación de servicio a baja tasa contra servidores.* Tesis Doctoral, Universidad de Granada.

Ramirez Walteros, Y. A. (2013). *Extracción de datos para la clasificación y filtrado de IPs falsas en ataques DDoS.* Duitama.

Tello Padilla, R. A. (2013). *Esquema de seguridad contra ataques DoS y DDoS, Caso: Diario Quintana Roo.* Tesis de Titulación, Universidad de Quintana Roo, México.

Valenzuela, P. (2008). *Una propuesta de IDS, basado en redes neuronales recurrentes.* Universidad de Santiago de Chile, Chile.

De la Hoz Correa, E. (2016). Mapas auto-organizativos probabilísticos y análisis en componentes de conexiones para la detección de anomalías en redes de computadores (Tesis Doctoral). Universidad de Granada, España.

Arbor Networks. Consultado en: http://es.arbornetworks.com/proteccion-ddos/

De la Hoz Correa, E. (2016). Mapas auto-organizativos probabilísticos y análisis en componentes de conexiones para la detección de anomalías en redes de computadores (Tesis Doctoral). Universidad de Granada, España.

Murillo, J. (2012). Métodos de investigación de enfoque experimental. Madrid: Universidad Autónoma de Madrid.

Zurutza, O. (2004). *Estado del arte de sistemas de detección de intrusos.* Escuela Politecnica Superior de Mondragón, España.

ANEXOS

Pruebas Servidor Web por Defecto

Tabla 8 Ataques DoS configuración por Defecto del Servidor Web – Parte 1

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
1	40000	10	20 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	675	0%
2	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
3	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
4	40000	10	25 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
5	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
6	40000	10	19 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
7	40000	10	19 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
8	40000	10	23 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
9	40000	10	22 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
10	40000	10	23 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
11	40000	10	25 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
12	40000	10	27 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
13	40000	10	23 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
14	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
15	40000	10	25 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%
16	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	614	0%
17	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
18	40000	10	25 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	601	0%
19	40000	10	21 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	608	0%
20	40000	10	19 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
21	40000	10	19 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
22	40000	10	23 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
23	40000	10	22 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
24	40000	10	23 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
25	40000	10	25 min	100.86.41.134	tesiscafe.sytes.net	100.86.52.5	0	0	10	711	0%
26	40000	10	27 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	710	0%
27	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
28	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
29	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
30	40000	10	20 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
31	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
32	40000	10	22 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%
33	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	614	0%
34	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	599	0%
35	40000	10	20 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
36	40000	10	21 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
37	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
38	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
39	40000	10	20 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
40	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
41	40000	10	22 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
42	40000	10	23 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
43	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
44	40000	10	20 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
45	40000	10	21 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%
46	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	614	0%
47	40000	10	25 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	599	0%
48	40000	10	21 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
49	40000	10	20 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
50	40000	10	26 min	100.86.21.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%

Tabla 9 Ataques DoS configuración por Defecto del Servidor Web – Parte 2

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
51	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
52	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
53	40000	10	19 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
54	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
55	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
56	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
57	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
58	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
59	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
60	40000	10	22 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
61	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
62	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
63	40000	10	27 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
64	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
65	40000	10	22 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
66	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
67	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
68	40000	10	19 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
69	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
70	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
71	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%
72	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	614	0%
73	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
74	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	601	0%
75	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	608	0%
76	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	675	0%
77	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
78	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
79	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
80	40000	10	25 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
81	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
82	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	675	0%
83	40000	10	25 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
84	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
85	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
86	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
87	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
88	40000	10	24 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
89	40000	10	26 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
90	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
91	40000	10	19 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
92	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
93	40000	10	26 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
94	40000	10	23 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	632	0%
95	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
96	40000	10	24 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	641	0%
97	40000	10	24 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	614	0%
98	40000	10	26 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
99	40000	10	20 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	601	0%
100	40000	10	21 min	100.86.84.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	608	0%

Tabla 10 Ataques DoS configuración por Defecto del Servidor Web – Parte 3

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
101	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
102	40000	10	25 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
103	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
104	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
105	40000	10	25 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
106	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
107	40000	10	23 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
108	40000	10	20 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
109	40000	10	23 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
110	40000	10	22 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
111	40000	10	23 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
112	40000	10	25 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
113	40000	10	27 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
114	40000	10	19 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
115	40000	10	22 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
116	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	654	0%
117	40000	10	25 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	623	0%
118	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
119	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
120	40000	10	25 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
121	40000	10	21 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
122	40000	10	20 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
123	40000	10	23 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
124	40000	10	20 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
125	40000	10	23 min	100.86.45.62	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
126	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
127	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
128	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
129	40000	10	19 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
130	40000	10	25 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
131	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
132	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
133	40000	10	25 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
134	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
135	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
136	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
137	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
138	40000	10	24 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
139	40000	10	26 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
140	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
141	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
142	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
143	40000	10	26 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
144	40000	10	19 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
145	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
146	40000	10	24 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
147	40000	10	24 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	625	0%
148	40000	10	19 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
149	40000	10	20 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
150	40000	10	21 min	100.86.68.32	tesiscafe.sytes.net	100.86.52.5	0	0	10	711	0%

Tabla 11 Ataques DoS configuración por Defecto del Servidor Web – Parte 4

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
151	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
152	40000	10	25 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
153	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
154	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
155	40000	10	25 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
156	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
157	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
158	40000	10	20 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
159	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
160	40000	10	22 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
161	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
162	40000	10	25 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
163	40000	10	27 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
164	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
165	40000	10	22 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
166	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
167	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
168	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
169	40000	10	25 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
170	40000	10	21 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
171	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
172	40000	10	20 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
173	40000	10	23 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
174	40000	10	22 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
175	40000	10	27 min	100.86.85.24	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
176	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
177	40000	10	22 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
178	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
179	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
180	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
181	40000	10	25 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
182	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
183	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
184	40000	10	20 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
185	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
186	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
187	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
188	40000	10	25 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
189	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
190	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
191	40000	10	20 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
192	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
193	40000	10	22 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
194	40000	10	23 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
195	40000	10	24 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
196	40000	10	26 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
197	40000	10	24 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
198	40000	10	26 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
199	40000	10	20 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
200	40000	10	21 min	100.86.44.77	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%

Tabla 12 Ataques DoS configuración por Defecto del Servidor Web – Parte 5

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
201	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
202	40000	10	25 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
203	40000	10	19 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
204	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
205	40000	10	25 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
206	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
207	40000	10	23 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
208	40000	10	20 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
209	40000	10	23 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
210	40000	10	22 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
211	40000	10	23 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
212	40000	10	25 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
213	40000	10	27 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
214	40000	10	19 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
215	40000	10	22 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
216	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
217	40000	10	25 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
218	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
219	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
220	40000	10	25 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
221	40000	10	21 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
222	40000	10	20 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
223	40000	10	23 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
224	40000	10	20 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
225	40000	10	23 min	100.86.49.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
226	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
227	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
228	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
229	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
230	40000	10	25 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
231	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
232	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
233	40000	10	25 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
234	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
235	40000	10	19 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
236	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
237	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
238	40000	10	24 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
239	40000	10	26 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
240	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
241	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
242	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
243	40000	10	26 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
244	40000	10	23 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
245	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
246	40000	10	24 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
247	40000	10	19 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
248	40000	10	26 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
249	40000	10	20 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
250	40000	10	21 min	100.86.46.120	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%

Tabla 13 Ataques DoS configuración por Defecto del Servidor Web – Parte 6

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
251	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
252	40000	10	25 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
253	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
254	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
255	40000	10	25 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
256	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
257	40000	10	23 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
258	40000	10	20 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
259	40000	10	23 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
260	40000	10	22 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
261	40000	10	23 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
262	40000	10	25 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
263	40000	10	19 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
264	40000	10	23 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
265	40000	10	19 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
266	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
267	40000	10	25 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
268	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
269	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
270	40000	10	25 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
271	40000	10	21 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
272	40000	10	20 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
273	40000	10	23 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
274	40000	10	20 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
275	40000	10	19 min	100.86.44.92	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
276	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
277	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
278	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
279	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
280	40000	10	25 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
281	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
282	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
283	40000	10	25 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
284	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
285	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
286	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
287	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
288	40000	10	24 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
289	40000	10	18 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	50	0%
290	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
291	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
292	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
293	40000	10	26 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
294	40000	10	23 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
295	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
296	40000	10	24 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
297	40000	10	24 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
298	40000	10	26 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
299	40000	10	20 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
300	40000	10	21 min	100.86.8.130	tesiscafe.sytes.net	100.86.52.5	0	0	10	689	0%

Tabla 14 Ataques DoS configuración por Defecto del Servidor Web – Parte 7

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
301	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
302	40000	10	25 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
303	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
304	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
305	40000	10	25 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
306	40000	10	19 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
307	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
308	40000	10	20 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
309	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
310	40000	10	22 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
311	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
312	40000	10	19 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
313	40000	10	27 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
314	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
315	40000	10	22 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
316	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
317	40000	10	25 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
318	40000	10	19 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
319	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
320	40000	10	25 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
321	40000	10	21 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
322	40000	10	20 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
323	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
324	40000	10	20 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
325	40000	10	23 min	100.86.32.121	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
326	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
327	40000	10	19 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
328	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
329	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
330	40000	10	25 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
331	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
332	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
333	40000	10	25 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
334	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
335	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
336	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
337	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
338	40000	10	24 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
339	40000	10	26 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
340	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
341	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
342	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
343	40000	10	26 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
344	40000	10	23 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
345	40000	10	19 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
346	40000	10	24 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
347	40000	10	19 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
348	40000	10	26 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
349	40000	10	20 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
350	40000	10	21 min	100.86.47.82	tesiscafe.sytes.net	100.86.52.5	0	0	10	715	0%

Tabla 15 Ataques DoS configuración por Defecto del Servidor Web – Parte 8

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
351	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
352	40000	10	25 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
353	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
354	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
355	40000	10	25 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
356	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
357	40000	10	19 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
358	40000	10	19 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
359	40000	10	23 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
360	40000	10	22 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
361	40000	10	23 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
362	40000	10	25 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
363	40000	10	27 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
364	40000	10	23 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
365	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
366	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
367	40000	10	25 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
368	40000	10	21 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
369	40000	10	19 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
370	40000	10	19 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
371	40000	10	23 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
372	40000	10	22 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
373	40000	10	23 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
374	40000	10	25 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	714	0%
375	40000	10	27 min	100.86.52.64	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
376	40000	10	23 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
377	40000	10	20 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
378	40000	10	20 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
379	40000	10	21 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
380	40000	10	25 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%
381	40000	10	21 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	645	0%
382	40000	10	21 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	633	0%
383	40000	10	25 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	712	0%
384	40000	10	21 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	713	0%
385	40000	10	20 min	100.86.12.126	tesiscafe.sytes.net	100.86.52.5	0	0	10	671	0%

Pruebas Servidor Web – Mod_evasive – Mod_security

Tabla 16 Ataques DoS configuración Mod_evasive – Mod_security – Parte 1

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones Legitimas	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
1	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39708	1	9	292	10%
2	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39780	0	10	220	0%
3	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
4	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
5	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
6	40000	10	26 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
7	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39809	3	7	191	30%
8	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
9	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39670	0	10	330	0%
10	40000	10	22 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39775	0	10	225	0%
11	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39717	0	10	283	0%
12	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
13	40000	10	27 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
14	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
15	40000	10	22 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
16	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
17	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
18	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39700	3	7	300	30%
19	40000	10	25 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39737	0	10	263	0%
20	40000	10	21 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39725	0	10	275	0%
21	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
22	40000	10	26 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39673	0	10	327	0%
23	40000	10	23 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39780	2	8	220	20%
24	40000	10	20 min	100.86.47.24	tesiscafe.sytes.net	190.42.88.79	39703	0	10	297	0%
25	40000	10	23 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
26	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
27	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39759	1	9	241	10%
28	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39786	0	10	214	0%
29	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
30	40000	10	25 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39795	0	10	205	0%
31	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39786	1	9	214	10%
32	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39695	0	10	305	0%
33	40000	10	25 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39692	0	10	308	0%
34	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
35	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39775	1	9	225	10%
36	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39808	0	10	192	0%
37	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39780	0	10	220	0%
38	40000	10	25 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39673	0	10	327	0%
39	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39734	2	8	266	20%
40	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
41	40000	10	26 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39666	0	10	334	0%
42	40000	10	23 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39780	0	10	220	0%
43	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39714	0	10	286	0%
44	40000	10	23 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39746	1	9	254	10%
45	40000	10	24 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39717	1	9	283	10%
46	40000	10	24 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
47	40000	10	24 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
48	40000	10	26 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39747	0	10	253	0%
49	40000	10	20 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39779	0	10	221	0%
50	40000	10	21 min	100.86.8.24	tesiscafe.sytes.net	190.42.88.79	39786	3	7	214	30%

Tabla 17 Ataques DoS configuración Mod_evasive – Mod_security – Parte 2

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
51	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39708	2	8	292	20%
52	40000	10	25 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39780	0	10	220	0%
53	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
54	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
55	40000	10	25 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
56	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
57	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39809	3	7	191	30%
58	40000	10	20 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
59	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39670	0	10	330	0%
60	40000	10	22 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39775	0	10	225	0%
61	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39717	0	10	283	0%
62	40000	10	25 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
63	40000	10	27 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
64	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
65	40000	10	22 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
66	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39740	1	9	260	10%
67	40000	10	25 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
68	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
69	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39737	0	10	263	0%
70	40000	10	25 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39725	0	10	275	0%
71	40000	10	21 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
72	40000	10	20 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39673	0	10	327	0%
73	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39780	0	10	220	0%
74	40000	10	20 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39703	0	10	297	0%
75	40000	10	23 min	100.86.62.84	tesiscafe.sytes.net	190.42.88.79	39738	3	7	262	30%
76	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39745	1	9	255	10%
77	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39759	0	10	241	0%
78	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
79	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
80	40000	10	25 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
81	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
82	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39809	3	7	191	30%
83	40000	10	25 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39802	1	9	198	10%
84	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39670	0	10	330	0%
85	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
86	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
87	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
88	40000	10	24 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
89	40000	10	26 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39809	3	7	191	30%
90	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
91	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39670	0	10	330	0%
92	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39775	0	10	225	0%
93	40000	10	26 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39717	0	10	283	0%
94	40000	10	23 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
95	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
96	40000	10	24 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
97	40000	10	24 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
98	40000	10	26 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
99	40000	10	20 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
100	40000	10	21 min	100.86.44.32	tesiscafe.sytes.net	190.42.88.79	39700	3	7	300	30%

Tabla 18 Ataques DoS configuración Mod_evasive – Mod_security – Parte 3

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
101	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39800	3	7	200	30%
102	40000	10	25 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39797	2	8	203	20%
103	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
104	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
105	40000	10	25 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39744	0	10	256	0%
106	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39746	0	10	254	0%
107	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
108	40000	10	20 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39794	0	10	206	0%
109	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
110	40000	10	22 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39800	1	9	200	10%
111	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
112	40000	10	25 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
113	40000	10	27 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39809	3	7	191	30%
114	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39802	2	8	198	20%
115	40000	10	22 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39670	0	10	330	0%
116	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39775	0	10	225	0%
117	40000	10	25 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39717	0	10	283	0%
118	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39726	3	7	274	30%
119	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
120	40000	10	25 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
121	40000	10	21 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
122	40000	10	20 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
123	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
124	40000	10	20 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
125	40000	10	23 min	100.86.38.8	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
126	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39797	3	7	203	30%
127	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39675	2	8	325	20%
128	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
129	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39744	0	10	256	0%
130	40000	10	25 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39746	0	10	254	0%
131	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
132	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
133	40000	10	25 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39797	0	10	203	0%
134	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
135	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39799	1	9	201	10%
136	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39744	1	9	256	10%
137	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39800	1	9	200	10%
138	40000	10	24 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39797	1	9	203	10%
139	40000	10	26 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39675	1	9	325	10%
140	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
141	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39797	0	10	203	0%
142	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
143	40000	10	26 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
144	40000	10	23 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39744	0	10	256	0%
145	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39746	0	10	254	0%
146	40000	10	24 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
147	40000	10	24 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39794	2	8	206	20%
148	40000	10	26 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%
149	40000	10	20 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
150	40000	10	21 min	100.86.32.45	tesiscafe.sytes.net	190.42.88.79	39799	1	9	201	10%

Tabla 19 Ataques DoS configuración Mod_evasive – Mod_security – Parte 4

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
151	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39805	1	9	195	10%
152	40000	10	25 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39794	0	10	206	0%
153	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	37986	0	10	2014	0%
154	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39744	0	10	256	0%
155	40000	10	25 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
156	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
157	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39699	3	7	301	30%
158	40000	10	20 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
159	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
160	40000	10	22 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39724	1	9	276	10%
161	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
162	40000	10	25 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
163	40000	10	27 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
164	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
165	40000	10	22 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
166	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39740	3	7	260	30%
167	40000	10	25 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
168	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
169	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
170	40000	10	25 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39797	0	10	203	0%
171	40000	10	21 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39675	2	8	325	20%
172	40000	10	20 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
173	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
174	40000	10	20 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
175	40000	10	23 min	100.86.6.24	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
176	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
177	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39740	3	7	260	30%
178	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
179	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
180	40000	10	25 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
181	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
182	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39699	2	8	301	20%
183	40000	10	25 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
184	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
185	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
186	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39700	1	9	300	10%
187	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
188	40000	10	24 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
189	40000	10	26 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
190	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
191	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
192	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
193	40000	10	26 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
194	40000	10	23 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39800	0	10	200	0%
195	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39797	1	9	203	10%
196	40000	10	24 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39675	0	10	325	0%
197	40000	10	24 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
198	40000	10	26 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39744	2	8	256	20%
199	40000	10	20 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39746	0	10	254	0%
200	40000	10	21 min	100.86.64.9	tesiscafe.sytes.net	190.42.88.79	39801	0	10	199	0%

Tabla 20 Ataques DoS configuración Mod_evasive – Mod_security – Parte 5

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
201	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39799	2	8	201	20%
202	40000	10	25 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
203	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
204	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
205	40000	10	25 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
206	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
207	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39724	3	7	276	30%
208	40000	10	20 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
209	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
210	40000	10	22 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
211	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
212	40000	10	25 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
213	40000	10	27 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
214	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
215	40000	10	22 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
216	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39724	2	8	276	20%
217	40000	10	25 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
218	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
219	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
220	40000	10	25 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
221	40000	10	21 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
222	40000	10	20 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39726	3	7	274	30%
223	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
224	40000	10	20 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
225	40000	10	23 min	100.86.44.21	tesiscafe.sytes.net	190.42.88.79	39738	2	8	262	20%
226	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
227	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
228	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
229	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
230	40000	10	25 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
231	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39699	3	7	301	30%
232	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39738	2	8	262	20%
233	40000	10	25 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
234	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
235	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
236	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
237	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
238	40000	10	24 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39738	3	7	262	30%
239	40000	10	26 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
240	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
241	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
242	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
243	40000	10	26 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
244	40000	10	23 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
245	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
246	40000	10	24 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
247	40000	10	24 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39724	1	9	276	10%
248	40000	10	26 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39785	0	10	215	0%
249	40000	10	20 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39797	0	10	203	0%
250	40000	10	21 min	100.86.36.8	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%

Tabla 21 Ataques DoS configuración Mod_evasive – Mod_security – Parte 6

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
251	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
252	40000	10	25 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
253	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
254	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
255	40000	10	25 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
256	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
257	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39726	3	7	274	30%
258	40000	10	20 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
259	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
260	40000	10	22 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
261	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
262	40000	10	25 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
263	40000	10	27 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
264	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
265	40000	10	22 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
266	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39724	1	9	276	10%
267	40000	10	25 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
268	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
269	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39745	3	7	255	30%
270	40000	10	25 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
271	40000	10	21 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
272	40000	10	20 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
273	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
274	40000	10	20 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
275	40000	10	23 min	100.86.23.16	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
276	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
277	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39745	3	7	255	30%
278	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
279	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
280	40000	10	25 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
281	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
282	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
283	40000	10	25 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
284	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
285	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
286	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
287	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39740	1	9	260	10%
288	40000	10	24 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
289	40000	10	26 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
290	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
291	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39699	1	9	301	10%
292	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
293	40000	10	26 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
294	40000	10	23 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39724	3	7	276	30%
295	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
296	40000	10	24 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
297	40000	10	24 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
298	40000	10	26 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
299	40000	10	20 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39737	2	8	263	20%
300	40000	10	21 min	100.86.36.18	tesiscafe.sytes.net	190.42.88.79	39802	0	10	198	0%

Tabla 22 Ataques DoS configuración Mod_evasive – Mod_security – Parte 7

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
301	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
302	40000	10	25 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
303	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
304	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39740	1	9	260	10%
305	40000	10	25 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
306	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
307	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39726	3	7	274	30%
308	40000	10	20 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
309	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
310	40000	10	22 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
311	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
312	40000	10	25 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
313	40000	10	27 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
314	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
315	40000	10	22 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
316	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39740	1	9	260	10%
317	40000	10	25 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
318	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
319	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39726	3	7	274	30%
320	40000	10	25 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
321	40000	10	21 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
322	40000	10	20 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
323	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
324	40000	10	20 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39799	2	8	201	20%
325	40000	10	23 min	100.86.14.26	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
326	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
327	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
328	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	1	9	255	10%
329	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
330	40000	10	25 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
331	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	3	7	301	30%
332	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
333	40000	10	25 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
334	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
335	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
336	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
337	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	3	7	255	30%
338	40000	10	24 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
339	40000	10	26 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
340	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
341	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
342	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39726	2	8	274	20%
343	40000	10	26 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
344	40000	10	23 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
345	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
346	40000	10	24 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39699	1	9	301	10%
347	40000	10	24 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
348	40000	10	26 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
349	40000	10	20 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
350	40000	10	21 min	100.86.24.47	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%

Tabla 23 Ataques DoS configuración Mod_evasive – Mod_security – Parte 8

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
351	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
352	40000	10	25 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39699	3	7	301	30%
353	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
354	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
355	40000	10	25 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
356	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
357	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
358	40000	10	20 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
359	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
360	40000	10	22 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
361	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39700	1	9	300	10%
362	40000	10	25 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
363	40000	10	27 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
364	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39699	3	7	301	30%
365	40000	10	22 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
366	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
367	40000	10	25 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
368	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
369	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39745	2	8	255	20%
370	40000	10	25 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
371	40000	10	21 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
372	40000	10	20 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
373	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
374	40000	10	20 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39724	0	10	276	0%
375	40000	10	23 min	100.86.23.32	tesiscafe.sytes.net	190.42.88.79	39700	2	8	300	20%
376	40000	10	21 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%
377	40000	10	20 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39745	0	10	255	0%
378	40000	10	20 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39699	0	10	301	0%
379	40000	10	21 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39738	0	10	262	0%
380	40000	10	25 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39740	1	9	260	10%
381	40000	10	21 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39799	0	10	201	0%
382	40000	10	21 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39740	0	10	260	0%
383	40000	10	25 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39724	3	7	276	30%
384	40000	10	21 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39700	0	10	300	0%
385	40000	10	20 min	100.86.21.33	tesiscafe.sytes.net	190.42.88.79	39726	0	10	274	0%

Pruebas Servidor Web – Snort + IPTables

Tabla 24 Ataques DoS configuración Snort + IPTables – Parte 1

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
1	40000	10	20 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
2	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
3	40000	10	25 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
4	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
5	40000	10	20 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
6	40000	10	26 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
7	40000	10	23 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
8	40000	10	20 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
9	40000	10	19 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
10	40000	10	22 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
11	40000	10	23 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
12	40000	10	25 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
13	40000	10	27 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
14	40000	10	23 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
15	40000	10	22 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
16	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
17	40000	10	25 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
18	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
19	40000	10	25 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
20	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
21	40000	10	20 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
22	40000	10	26 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
23	40000	10	23 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
24	40000	10	20 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
25	40000	10	23 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
26	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
27	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
28	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
29	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
30	40000	10	25 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
31	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
32	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
33	40000	10	25 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
34	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
35	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
36	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
37	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
38	40000	10	25 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
39	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
40	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
41	40000	10	26 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
42	40000	10	23 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
43	40000	10	20 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
44	40000	10	23 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
45	40000	10	24 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
46	40000	10	24 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
47	40000	10	24 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
48	40000	10	26 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
49	40000	10	19 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
50	40000	10	21 min	100.86.10.29	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 25 Ataques DoS configuración Snort + IPTables – Parte 2

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
51	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
52	40000	10	19 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
53	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
54	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
55	40000	10	25 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
56	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
57	40000	10	23 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
58	40000	10	20 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
59	40000	10	19 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
60	40000	10	22 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
61	40000	10	23 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
62	40000	10	25 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
63	40000	10	27 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
64	40000	10	23 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
65	40000	10	22 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
66	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
67	40000	10	25 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
68	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
69	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
70	40000	10	25 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
71	40000	10	21 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
72	40000	10	20 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39939	7	3	61	70%
73	40000	10	23 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
74	40000	10	20 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
75	40000	10	23 min	100.86.15.37	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
76	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
77	40000	10	19 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
78	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
79	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
80	40000	10	25 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
81	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
82	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
83	40000	10	25 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
84	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
85	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
86	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
87	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
88	40000	10	24 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
89	40000	10	26 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
90	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
91	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
92	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
93	40000	10	26 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
94	40000	10	23 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
95	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
96	40000	10	19 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
97	40000	10	24 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
98	40000	10	26 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
99	40000	10	20 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
100	40000	10	21 min	100.86.37.52	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 26 Ataques DoS configuración Snort + IPTables – Parte 3

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
101	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
102	40000	10	25 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
103	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
104	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
105	40000	10	25 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
106	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
107	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
108	40000	10	19 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
109	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
110	40000	10	22 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
111	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
112	40000	10	25 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39935	6	4	65	60%
113	40000	10	27 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
114	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
115	40000	10	22 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
116	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
117	40000	10	25 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
118	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
119	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
120	40000	10	25 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
121	40000	10	21 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
122	40000	10	20 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39925	7	3	75	70%
123	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
124	40000	10	20 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
125	40000	10	23 min	100.86.20.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
126	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
127	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
128	40000	10	19 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
129	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
130	40000	10	25 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
131	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
132	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
133	40000	10	25 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
134	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
135	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
136	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
137	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
138	40000	10	24 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
139	40000	10	26 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
140	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
141	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
142	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
143	40000	10	19 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
144	40000	10	23 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
145	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
146	40000	10	24 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
147	40000	10	24 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
148	40000	10	26 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
149	40000	10	20 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
150	40000	10	21 min	100.86.16.43	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 27 Ataques DoS configuración Snort + IPTables – Parte 4

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
151	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
152	40000	10	25 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
153	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
154	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
155	40000	10	25 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
156	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
157	40000	10	23 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
158	40000	10	20 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
159	40000	10	23 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
160	40000	10	22 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
161	40000	10	23 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
162	40000	10	25 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
163	40000	10	27 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
164	40000	10	19 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
165	40000	10	22 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
166	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
167	40000	10	25 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
168	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
169	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
170	40000	10	19 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
171	40000	10	21 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
172	40000	10	20 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39935	7	3	65	70%
173	40000	10	23 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
174	40000	10	20 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
175	40000	10	23 min	100.86.76.7	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
176	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
177	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
178	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
179	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
180	40000	10	25 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
181	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
182	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
183	40000	10	25 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
184	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
185	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
186	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
187	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
188	40000	10	24 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
189	40000	10	26 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
190	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
191	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
192	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
193	40000	10	26 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
194	40000	10	23 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
195	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
196	40000	10	24 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
197	40000	10	19 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
198	40000	10	26 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
199	40000	10	20 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
200	40000	10	21 min	100.86.33.151	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 28 Ataques DoS configuración Snort + IPTables – Parte 5

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del atague	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
201	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
202	40000	10	25 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
203	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
204	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
205	40000	10	25 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
206	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
207	40000	10	23 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
208	40000	10	20 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
209	40000	10	19 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
210	40000	10	22 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
211	40000	10	23 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
212	40000	10	25 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
213	40000	10	27 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
214	40000	10	23 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
215	40000	10	22 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
216	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
217	40000	10	25 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
218	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
219	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
220	40000	10	25 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
221	40000	10	21 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
222	40000	10	20 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39884	7	3	116	70%
223	40000	10	23 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
224	40000	10	20 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
225	40000	10	23 min	100.86.66.14	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
226	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
227	40000	10	19 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
228	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
229	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
230	40000	10	25 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
231	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
232	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
233	40000	10	19 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
234	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
235	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
236	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
237	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
238	40000	10	24 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
239	40000	10	26 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
240	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
241	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
242	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
243	40000	10	26 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
244	40000	10	23 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
245	40000	10	19 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
246	40000	10	24 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
247	40000	10	24 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
248	40000	10	26 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
249	40000	10	20 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
250	40000	10	21 min	100.86.20.35	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 29 Ataques DoS configuración Snort + IPTables – Parte 6

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
251	40000	10	19 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
252	40000	10	25 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
253	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
254	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
255	40000	10	25 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
256	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
257	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
258	40000	10	20 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
259	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
260	40000	10	22 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
261	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
262	40000	10	25 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
263	40000	10	27 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
264	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
265	40000	10	22 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
266	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
267	40000	10	19 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
268	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
269	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
270	40000	10	25 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
271	40000	10	21 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
272	40000	10	20 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39939	7	3	61	70%
273	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
274	40000	10	20 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
275	40000	10	23 min	100.86.14.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
276	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
277	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
278	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
279	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
280	40000	10	25 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
281	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
282	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
283	40000	10	25 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
284	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
285	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
286	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
287	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
288	40000	10	24 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
289	40000	10	26 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
290	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
291	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
292	40000	10	19 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
293	40000	10	26 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
294	40000	10	23 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
295	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
296	40000	10	24 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
297	40000	10	24 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
298	40000	10	26 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
299	40000	10	20 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
300	40000	10	21 min	100.86.61.15	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 30 Ataques DoS configuración Snort + IPTables – Parte 7

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
301	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
302	40000	10	25 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
303	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
304	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
305	40000	10	25 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
306	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
307	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
308	40000	10	20 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
309	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
310	40000	10	22 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
311	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
312	40000	10	25 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39868	6	4	132	60%
313	40000	10	27 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
314	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
315	40000	10	22 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
316	40000	10	19 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
317	40000	10	25 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
318	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
319	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
320	40000	10	25 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
321	40000	10	21 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
322	40000	10	20 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39884	7	3	116	70%
323	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
324	40000	10	20 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
325	40000	10	23 min	100.86.44.22	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
326	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
327	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
328	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
329	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
330	40000	10	25 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
331	40000	10	19 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
332	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
333	40000	10	25 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
334	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
335	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
336	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39922	10	0	78	100%
337	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
338	40000	10	24 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
339	40000	10	26 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
340	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
341	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
342	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
343	40000	10	19 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
344	40000	10	23 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
345	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39925	9	1	75	90%
346	40000	10	24 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
347	40000	10	24 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
348	40000	10	26 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
349	40000	10	20 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
350	40000	10	21 min	100.86.9.16	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

Tabla 31 Ataques DoS configuración Snort + IPTables – Parte 8

Fuente: Elaboración Propia

	HTTP ATTACK	Peticiones Legitimas	Duracion del ataque	Metodo de acceso			Variables				
Numero de Ataques	Numero de peticiones DoS	Numero de peticiones L	H:M:S	IP Servidor	Dominio servidor	IP Atacante	Verdaderos Positivos	Verdaderos Negativos	Falsos Positivos	Falsos Negativos	Disponibilidad del Servidor
351	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
352	40000	10	19 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	7	3	50	70%
353	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
354	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
355	40000	10	25 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
356	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
357	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
358	40000	10	20 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39932	9	1	68	90%
359	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
360	40000	10	22 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
361	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
362	40000	10	25 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	6	4	50	60%
363	40000	10	27 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
364	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	8	2	50	80%
365	40000	10	22 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
366	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
367	40000	10	25 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
368	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	9	1	50	90%
369	40000	10	19 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
370	40000	10	25 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39932	10	0	68	100%
371	40000	10	21 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
372	40000	10	20 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39884	7	3	116	70%
373	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
374	40000	10	20 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
375	40000	10	23 min	100.86.6.25	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
376	40000	10	21 min	100.86.6.72	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
377	40000	10	20 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
378	40000	10	20 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
379	40000	10	21 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
380	40000	10	25 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
381	40000	10	21 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
382	40000	10	21 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
383	40000	10	25 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
384	40000	10	21 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%
385	40000	10	20 min	100.86.54.21	tesiscafe.sytes.net	190.42.87.118	39950	10	0	50	100%

ACTA DE SUSTENTACIÓN

En la sala de sustentaciones de la Facultad de Ingeniería Civil, de Sistemas y de Arquitect
siendo las 10:45 am del día 21 de marzo del 2018, se reunieron los miembros del jurado de la tes
titulada: "PROTOTIPO DE DETECCION Y MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS), E
SERVIDORES WEB (Código IS-2016-087)". Conformado por los siguientes docentes:

M.A. Ing. Robert Edgar Puican Gutierrez	- Presidente
M.Sc. Gilberto Martín Ampuero Pasco	- Miembro
Ing. César Augusto Guzmán Valle	- Miembro
Mg. Ing. Juan Elías Villegas Cubas	- Patrocinador

Actuando como Presidente del jurado el M.A. Ing. Robert Edgar Puican Gutierrez y como secretario e
Ing. César Augusto Guzmán Valle, se procedió a recepcionar la sustentación de la tesis a cargo d
Bachiller:

RANDY STEVE YESQUÉN RODRÍGUEZ

Durante la sustentación el jurado procedió a deliberar libre y reservadamente acordando aprobar
el calificativo de MUY BUENO.

Finalmente se procedió a dar lectura a la presente acta, firmando en señal de conformidad l
docentes que en ella intervinieron, dando por concluido dicho acto siendo las 11:45 am del m

M. A. Ing. ROBERT EDGAR PUICAN GUTIERREZ
PRESIDENTE

M. Sc. GILBERTO MARTÍN AMPUERO PAS
MIEMBRO

ING. CÉSAR AUGUSTO GUZMÁN VALLE
MIEMBRO

MG. ING. JUAN ELÍAS VILLEGAS CUBA
PATROCINADOR

"Año de la universalización de la salud".

CONSTANCIA DE APROBACION DE ORIGINALIDAD DE TESIS

Según Res. N° 659-2020-R

Yo, Juan Elias Villegas Cubas, **asesor de tesis del bachiller**:

YESQUEN RODRIGUEZ RANDY STEVE

TITULADA:

PROTOTIPO DE DETECCIÓN Y MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DOS), EN SERVIDORES WEB

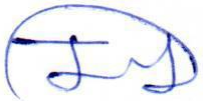
Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de **19**% verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, para la obtención de Gradosy Títulos de la UNPRG:

Lambayeque, 18 de julio del 2022

ATENTAMENTE,



Ing. Juan Elías Villegas Cubas
DNI. 80103991

Se adjunta:
Recibo digital de Turnitin
Revisión de informe en Turnitin

Prototipo de Detección Y Mitigación de Ataques de Denegación de Servicios (DoS), en Servidores Web

INFORME DE ORIGINALIDAD

19%	19%	2%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	2%
2	repositorio.unprg.edu.pe Fuente de Internet	2%
3	repositorio.uss.edu.pe Fuente de Internet	2%
4	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%
5	gist.github.com Fuente de Internet	1%
6	rootear.com Fuente de Internet	1%
7	kipdf.com Fuente de Internet	1%
8	www.redseguridad.com Fuente de Internet	1%

9	sedici.unlp.edu.ar Fuente de Internet	1 %
10	cso.computerworld.es Fuente de Internet	1 %
11	www.coursehero.com Fuente de Internet	1 %
12	securelist.lat Fuente de Internet	1 %
13	repositorio.unjbg.edu.pe Fuente de Internet	1 %
14	dtstc.ugr.es Fuente de Internet	<1 %
15	Submitted to Universidad Senor de Sipan Trabajo del estudiante	<1 %
16	digibug.ugr.es Fuente de Internet	<1 %
17	sublimerobots.com Fuente de Internet	<1 %
18	Submitted to UNITEC Institute of Technology Trabajo del estudiante	<1 %
19	alejandrooscaralexis.blogspot.com Fuente de Internet	<1 %
20	Submitted to Rochester Institute of Technology	<1 %

Trabajo del estudiante

21	repositorio.unprg.edu.pe:8080 Fuente de Internet	<1 %
22	fernandoloaiza14.blogspot.com Fuente de Internet	<1 %
23	dokumen.pub Fuente de Internet	<1 %
24	www.docstoc.com Fuente de Internet	<1 %
25	akavlankdage.wordpress.com Fuente de Internet	<1 %
26	informatica-0computacion.blogspot.com Fuente de Internet	<1 %
27	docplayer.es Fuente de Internet	<1 %
28	repositorio.uladech.edu.pe Fuente de Internet	<1 %

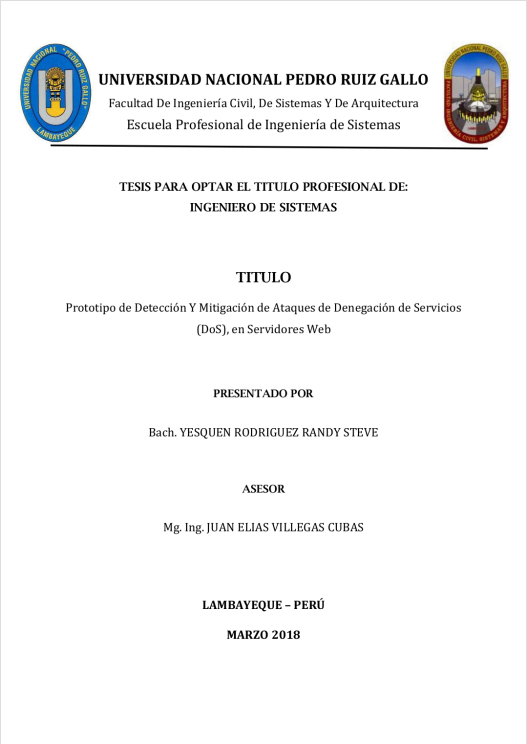
Excluir citas	Activo	Excluir coincidencias	< 20 words
Excluir bibliografía	Activo		

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Randy Steve Yesquen Rodriguez
Título del ejercicio:	TESIS
Título de la entrega:	Prototipo de Detección Y Mitigación de Ataques de Denegaci...
Nombre del archivo:	TESIS_RANDY.docx
Tamaño del archivo:	10.81M
Total páginas:	95
Total de palabras:	10,610
Total de caracteres:	57,999
Fecha de entrega:	18-jul.-2022 12:16p. m. (UTC-0500)
Identificador de la entre...	1872238425



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
Facultad De Ingeniería Civil, De Sistemas Y De Arquitectura
Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OPTAR EL TITULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

TITULO

Prototipo de Detección Y Mitigación de Ataques de Denegación de Servicios (DoS), en Servidores Web

PRESENTADO POR

Bach. YESQUEN RODRIGUEZ RANDY STEVE

ASESOR

Mg. Ing. JUAN ELIAS VILLEGAS CUBAS

LAMBAYEQUE – PERÚ

MARZO 2018