UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PREVENCIÓN Y DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDoS) IMPLEMENTANDO EL MÓDULO QOS EN EL SERVIDOR WEB APACHE"

TESIS

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS

PRESENTADA POR:

BACH. PAUL GIANCARLO LIZARES FIGUEROA

BACH. MARCO ANTONIO LÓPEZ BENAVIDES

ASESOR:

ING. JUAN ELÍAS VILLEGAS CUBAS

LAMBAYEQUE - PERÚ 2017

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"PREVENCIÓN Y DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDoS) IMPLEMENTANDO EL MÓDULO QOS EN EL SERVIDOR WEB APACHE"

RESPONSABLES:

Bach. PAUL GIANCARLO LIZARES FIGUEROA

Bach. MARCO ANTONIO LÓPEZ BENAVIDES

ASESOR:

ING. JUAN ELÍAS VILLEGAS CUBAS

Sustentada y Aprobada ante el honorable **Jurado**:

BERNARDO NÚÑEZ MONTENEGRO

ALBERTO ENRIQUE SAMILLÁN AYALA

ROBERTO CARLOS ARTEAGA LORA

LAMBAYEQUE - PERÚ 2017

DEDICATORIA

A mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento de mi capacidad.

Paul Giancarlo Lizares Figueroa

Dedico este proyecto a Dios por darme las fuerzas para lograr el desarrollo de este proyecto, a mis Padres, por permanecer conmigo siempre brindándome su apoyo incondicional para lograr mis objetivos

Marco Antonio López Benavides

AGRADECIMIENTO

En primer lugar, un agradecimiento especial a Dios, que nos guía, nos protege y nos da las fuerzas para avanzar en cada etapa de nuestra vida.

Agradezco a mis padres por su gran apoyo incondicional, por sus consejos, por todo el amor que me ofrecen día a día, por esa fortaleza que me brindan, todo ello suma constantemente para ser un profesional competitivo, con visión y agradecido con Dios.

Agradezco al lng. Juan Villegas Cubas, por su tiempo, sus consejos y su mano extendida siempre como amigo, docente, instructor y asesor, que permitieron el desarrollo del proyecto.

Y por último a todas las personas que contribuyeron con esta investigación.

Paul Giancarlo Lizares Figueroa

Agradezco a Dios por haber sido muy grato conmigo y rodearme de maravillosas personas y grandes amigos, amigos que siempre supieron dar su apoyo, tanto en lo personal, intelectual y laboral.

A nuestros padres por enseñarnos siempre que en la constancia está el éxito.

Agradecemos al lng. Juan Villegas Cubas por la confianza, orientación, y la paciencia depositada, que Dios lo bendiga.

Agradezco a todas las personas que directa o indirectamente intervinieron para la realización de este proyecto.

Marco Antonio López Benavides

RESUMEN

En este proyecto se pretende aplicar un módulo de seguridad de Apache que logre prevenir y detectar los ataques de denegación de servicio distribuido dirigidos al servidor web, el cual fue implementado en Apache y ejecutado en un sistema operativa Linux, teniendo como dominio propio a tesisseginf.sytes.net y cuya página web está diseñada para realizar las pruebas y demostraciones necesarias contra los ataques DDoS que se logran realizar gracias a la implementación de máquinas virtuales en diferentes equipos físicos cuyo sistema operativo es el Kali Linux, sistema principalmente encargado en seguridad y penetración en redes.

Para obtener los resultados se aplicó un diseño metodológico que permita someter nuestro objeto de estudio a dos procesos, el primero es el pre-test que se lleva a cabo cuando no es implementada nuestra solución y lograr evaluar el comportamiento al que es sometido el servidor sin ser protegido. El segundo proceso es el post-test que se lleva a cabo mediante la implementación de nuestra solución para luego analizar el comportamiento al que es sometido el servidor.

Todo el desarrollo del proyecto se llevó a cabo en un laboratorio propio que consiste por un lado del servidor web cuyo servicio es público a Internet durante el tiempo de prueba, ubicado en la casa de un integrante del proyecto y por otro lado los equipos atacantes conectados a Internet para lograr acceder a la página web, ubicado en la casa del otro integrante. Con la finalidad de lograr un escenario real el cual permitirá conocer como son afectadas empresas con este tipo de ataques.

Por último, la propuesta dada cumple con los requerimientos de seguridad y resultados esperados.

ABSTRACT

This project intends to apply an Apache security module to prevent and detect distributed denial of service attacks directed at the web server, which was implemented in Apache and executed in a Linux operating system, having as its own domain tesisseginf .sytes.net and whose web page is designed to perform the necessary tests and demonstrations against the DDoS attacks that are achieved thanks to the implementation of virtual machines in different physical equipment whose operating system is Kali Linux, system mainly in charge of security and penetration in networks.

To obtain the results we applied a methodological design that allows us to subject our study object to two processes. The first one is the pre-test that is carried out when our solution is not implemented and to be able to evaluate the behavior to which the server is submitted without be protected. The second process is the post-test that is carried out when our solution is implemented and analyze the behavior to which the server is subjected.

The entire development of the project was carried out in an own laboratory consisting of the web server whose service is public to the Internet during the test time, located in the house of a member of the project and on the other hand the attacking teams connected to the Internet to obtain access to the web page, located in the house of the other member. With the aim of achieving a real scenario which will allow to know how are affected companies with this type of attacks.

Finally, the given proposal meets the security requirements and expected results.

INTRODUCCIÓN

Hoy en día es común escuchar de ciberataques dirigidos principalmente a los servidores web y afectan a todo tipo de infraestructura, logrando que el servicio que brindan no esté disponible por algún tiempo o no responda a las peticiones solicitadas, estos ataques son conocidos como denegación de servicio distribuido, acción realizada por más de un atacante, logrando que incapacite el hardware, software o ambos de un servidor impidiendo tener el funcionamiento adecuado sin la posibilidad de responder a las peticiones. Se entiende como ataques de denegación de servicios distribuido al flujo masivo de peticiones dirigidas al servidor web a través del protocolo TCP/IP provenientes de redes remotas y en otros casos redes locales.

Con este antecedente es que se desarrolla este proyecto, teniendo como finalidad la detección y prevención de ataques de denegación de servicio distribuidos a servidores web Apache, esto permitirá que los servicios brindados por tales sitios web estén principalmente disponibles al momento de que cualquier usuario o cliente legítimo quiera acceder con lo cual conllevaría a la continuidad del negocio en el caso de ser implementado como herramienta de seguridad en una empresa.

La siguiente investigación se estructura en 7 capítulos los cuales son:

El Capítulo I: Marco Referencial, se presenta el planteamiento del problema, descripción del proyecto, hipótesis, objetivos, limitaciones, justificación e importancia.

El Capítulo II: Marco teórico, se describe la parte teórica sobre la que se sustenta la investigación como son los antecedentes y base teórica.

El Capítulo III: Marco metodológico, explicación de la metodología utilizada para el análisis de la problemática a desarrollar.

El Capítulo IV: Desarrollo de la propuesta

Capítulo V: Análisis y discusión de resultados.

Capítulo VI: Conclusiones y Recomendaciones.

Capítulo VII: Referencias bibliográficas.

LISTA DE FIGURAS

LISTA DE TABLAS

ÍNDICE

CAPÍTULO I

I. MARCO REFERENCIAL

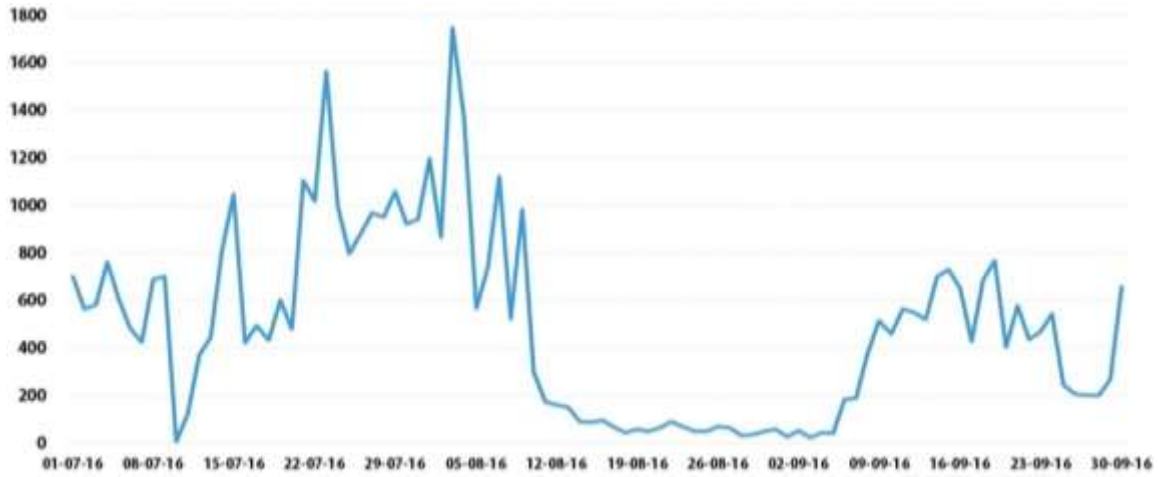
1.1. Situación Problemática

En la actualidad la ciberdelincuencia es un término muy común que vende como uno de sus servicios más populares el ataque DDoS (Distributed Denial of Service). Este tipo de ataque explota alguna vulnerabilidad en un sistema computarizado mediante los conocidos "ordenadores zombies" que crean un enorme flujo de solicitudes con la finalidad que el objetivo se sobrecargue y sea forzado a cerrarse, afectando a los verdaderos usuarios.

El "ataque distribuido de denegación de servicios" puede resultar perjudicial para una entidad ya que le genera pérdidas en la capacidad de comercializar, daños en su reputación, perdida de acceso a información crítica, perdidas en oportunidades de negocio, entre otros que pueden llevar a una organización a la quiebra de no tomarse las medidas correctivas correspondientes.

A continuación, se observa la frecuencia de los ataques DDoS en el último trimestre del 2016.

***Figura 1**: Frecuencia de ataques DDoS en el último trimestre del 2016*

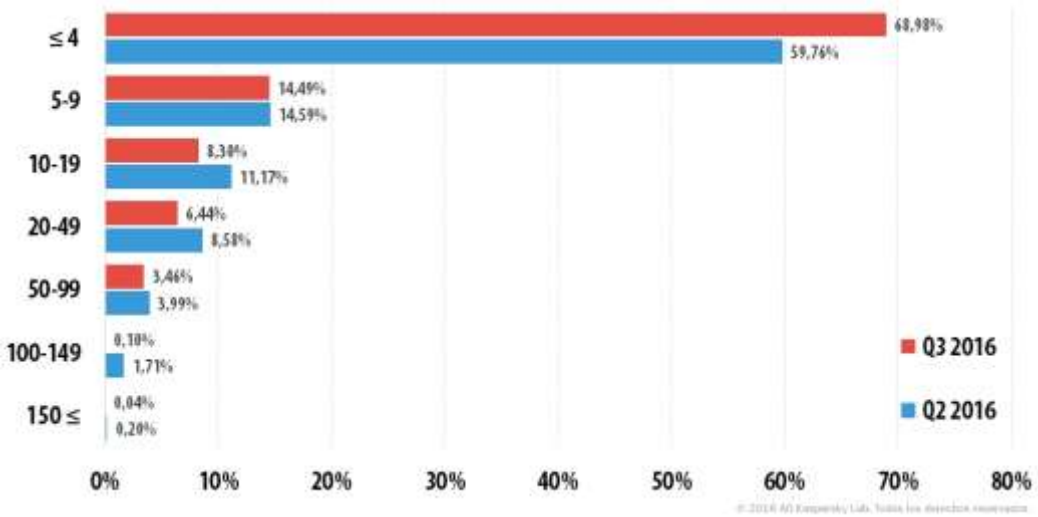


Fuente:

Khalimonenko, A. (31 de Octubre de 2016). *SECURELIST*. Obtenido de https://securelist.lat/analysis/informes-trimestrales-sobre-malware/84143/kaspersky-ddos-intelligence-report-for-q3-2016/

Además, la mayor frecuencia de duración de los ataques DDoS fue de <= 4 horas como se muestra a continuación.

Figura 2: *Tiempos de ataque DDoS menos a 4 horas más efectuados.*

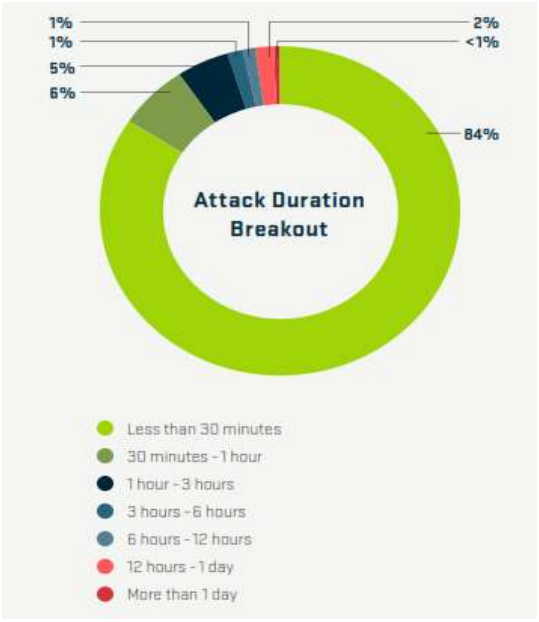


Fuente:

Khalimonenko, A. (31 de octubre de 2016). *SECURELIST*. Obtenido de https://securelist.lat/kaspersky-ddos-intelligence-report-for-q3-2016/84143/

En cuanto a la duración de ataques DDoS, también podemos mencionar que en su mayoría son aún menores de 4 horas como se mostró anteriormente. Podemos decir que la mayor frecuencia de duraciones de ataques DDoS de acuerdo al resultado siguiente son menores de 30 minutos.

Figura 3*: Tiempos de ataque DDoS menos de 30 minutos.*



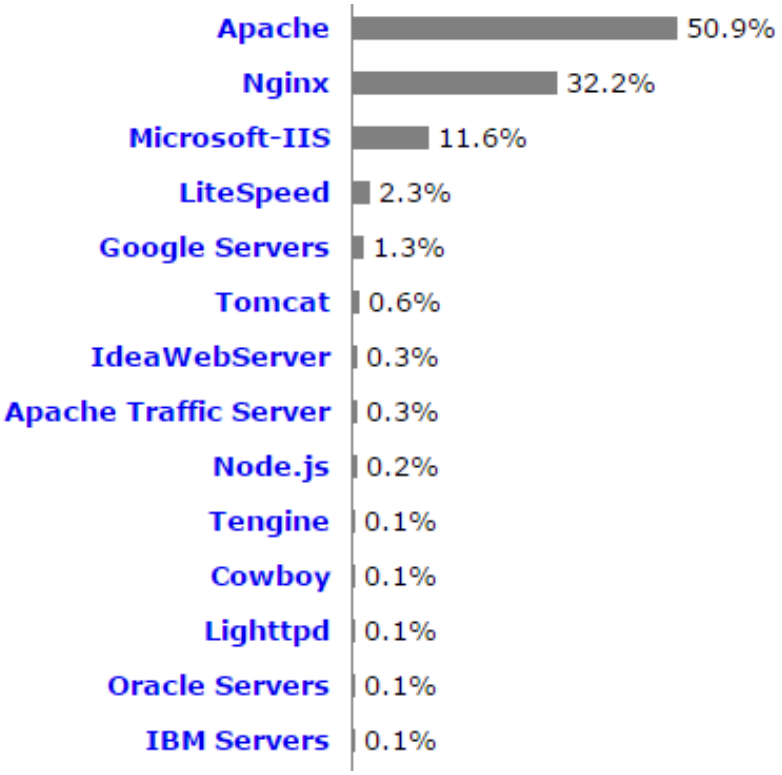
Fuente:

networks, a. (2016). worldwide infrastructure security report. *arbor networks*, 104.

Para contextualizar la problemática hablaremos de los servidores web Apache que serán parte de nuestra investigación debido a su alta aceptación en la red, su alta configuración y su desarrollo dentro de HTTP.

Para realizar un entorno ciertamente confiable hemos considerado uno de los ataques más efectivos y uno de los sistemas computarizados más populares y utilizados como los servidores web apache, como se demuestra a continuación:

Figura 4: *Servidor Web Apache más utilizado.*



Fuente:

W3Techs. (01 de Diciembre de 2016). *W3Techs*. Obtenido de https://w3techs.com/technologies/overview/web_server/all

Es importante entender cuan peligroso puede resultar para una organización este tipo de ciberataques y a su vez es vital poder detectar y prevenir estos ataques para evitar cuantiosas pérdidas corporativas.

1.2. Descripción del proyecto

En primer lugar, instalaremos el servidor web que estará bajo la distribución Ubuntu del sistema operativo Linux, este será expuesto a diversos ataques DDoS, mediante los cuales verificaremos que el servicio que brinda el servidor colapse y por ende el servicio no esté disponible durante el periodo de ataque.

Posteriormente aplicaremos el módulo de seguridad apache mod_qos, el cual nos servirá para detectar y prevenir los ataques de denegación de servicio distribuido dirigidos al servidor web, una vez instalado este módulo de seguridad se realizarán diversos ataques para garantizar que la solución es la óptima ante los ataques DDoS.

El servidor tendrá un dominio previamente configurado, que está diseñado para realizar las pruebas y demostraciones necesarias contra los ataques DDoS aplicadas al servidor web.

1.3. Formulación de la pregunta de investigación

¿Cómo prevenir y detectar los ataques DDoS en un servidor web Apache?

1.4. Hipótesis

Con la implementación del módulo de seguridad QoS se podrá prevenir y detectar ataques DDoS al servidor web Apache.

1.5. Objetivos

1.5.1. Objetivo General

Implementar el módulo de seguridad Apache mod_qos para prevenir y detectar ataques de tipo DDoS dirigidos al servidor web Apache.

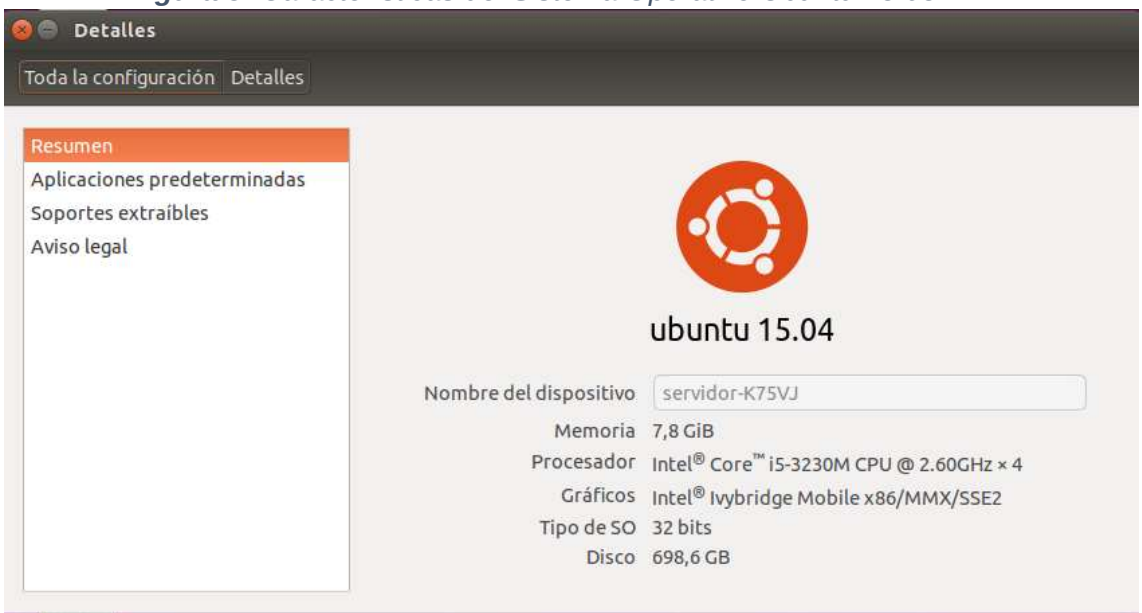
1.5.2. Objetivos Específicos

- Identificar los ataques de denegación de servicio distribuido en servidores web Apache.
- Implementar un servidor web Apache y verificar vulnerabilidades de DDoS.
- Analizar los módulos de seguridad de Apache que brindan protección contra los ataques DDoS
- Implementar el módulo de seguridad QoS en el servidor web Apache.
- Analizar resultados de prevención y detección de ataques DDoS en el módulo de seguridad QoS implementado.

1.6. Limitaciones

- Se utilizaron 4 ordenadores virtuales que cumplieron la función de “ordenadores zombies” para realizar los ataques.
- Sólo utilizamos ataques externos hacia el servidor web que se encuentra dentro de una DMZ (Zona Desmilitarizada).
- No se implementó en una empresa por las restricciones con las que cuentan para ser realizadas.
- Se llevó a cabo dentro de un laboratorio propio.

Figura 5: *Características del Sistema Operativo Ubuntu 15.05*



Fuente: Elaboración propia.

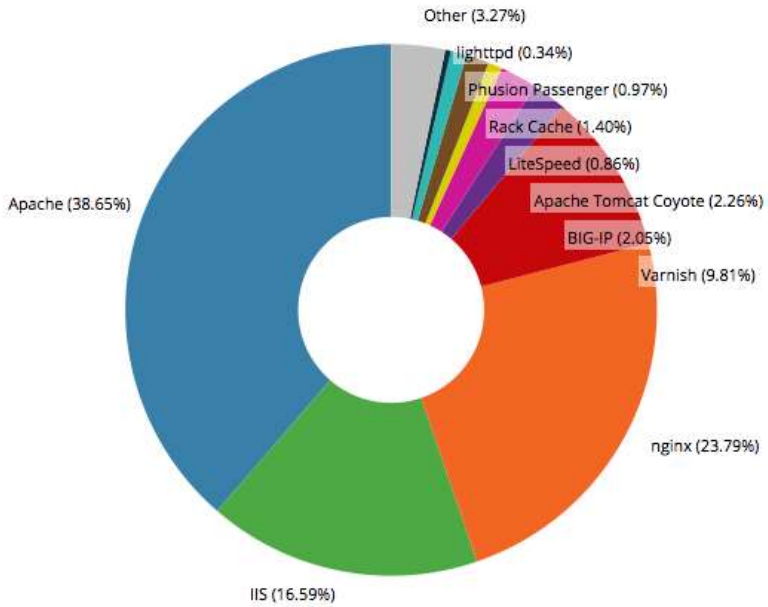
1.7. Justificación e Importancia

En la actualidad la seguridad informática es un factor primordial de cualquier empresa, todas las empresas están expuestas a diversas vulnerabilidades, los ataques DDoS buscan inutilizar sitios web y por tanto que dejen de prestar sus servicios en tiempo real.

Es aquí donde radica la importancia de la prevención y detección de los ataques DDoS para una organización, debido a que toda institución siempre busca mitigar al máximo sus riesgos, en el presente proyecto encontraremos un método de protección efectivo contra dichos ataques.

Utilizaremos un servidor Apache en el cual cargaremos el sitio web http://tesisseginf.sytes.net. En particular utilizamos un servidor Apache producto de que es el servidor más utilizado y el más popular a nivel mundial como se demuestra a continuación:

Figura 6: *Diferencias de uso entre servidores web.*



Fuente:

Velneo. (2015 de Septiembre de 2015). *Velneo*. Obtenido de https://velneo.es/lenguajes-de-programacion-mas-demandados-en-2015/

Es importante recalcar que la mayoría de los ordenadores contienen información sensible a vulnerabilidades informáticas y por ende las instituciones están inmersas a diversos riesgos como pérdida de oportunidades de negocio, producto de no tener los recursos habilitados en tiempo real. Puede afectar la reputación y disminuir la capacidad comercial de la entidad.

Podemos concluir que los ataques DDoS pueden tener efectos devastadores para las instituciones que no cuentan con un método apropiado de protección ante este tipo de vulnerabilidades.

CAPÍTULO II

II. MARCO TEÓRICO

2.1. Antecedentes de otras investigaciones

1. Tello Padilla, R. A. (2013).

   “Luego de implementar las herramientas de mitigación de ataques DDoS queda claro que el apache mod evasive bloquea los ataques al puerto 80 y redirige al error 403. Aunque esta herramienta logra mitigar ataques hasta cierto grado, no será posible lograr defenderse ante un ataque más sofisticado utilizando BotNets; para lograr eso es necesario tener el respaldo de un gran ancho de banda y un entorno de servidores balanceados y distribuidos que logren recibir y soportar las peticiones en masa y al mismo tiempo de quizá cientos o miles de usuarios. Sin embargo, en mi experiencia puedo decir que, aunque la aplicación web de noticias del Diario de Quintana Roo recibe un promedio de 10580 visitantes distintos al día, estos no se conectan al mismo tiempo y los ataques del tipo DDoS recibidos hasta el momento no han sido muy complejos.”

2. Campo Giralte, L. (2009).

   “Se exploran soluciones a la denegación de servicio a nivel de aplicación. Para ello, se han estudiado e investigado técnicas basadas en redes neuronales, en análisis estadísticos a nivel IP, en correlación de flags TCP, en el estudio de comportamientos del usuario sobre los recursos del servidor, soluciones de control de flujo y en soluciones distribuidas, entre otras.

   El resultado de las técnicas estudiadas ha dado lugar a una solución distribuida, escalable y de bajo coste, dependiente del tipo de infraestructura que se quiere proteger. La propuesta considera una arquitectura distribuida basada en tres pilares fundamentales,

detección, comunicación y mitigación de la denegación de servicio. Dichos elementos, cooperan entre sí de manera que, tanto en datos reales y simulados, conseguimos detectar, mitigar y comunicar este tipo de ciberataques. Para la detección proponemos el empleo de un algoritmo que aporta elevadas tasas de detección en el protocolo HTTP. Por otra parte, mediante el uso de canales encubiertos conseguimos comunicar los diferentes elementos de la arquitectura propuesta de forma prácticamente invisible. Finalmente, conseguimos mitigar dichas intrusiones de manera que los usuarios habituales del servicio no experimenten ninguna alteración en sus comunicaciones.

Lo expuesto en la presente tesis funciona bajo cualquier sistema Linux y, si se quisiera, podría utilizarse en sistemas comerciales con la finalidad de garantizar la protección de aquellos usuarios de medianas empresas que no pueden asumir los costes de sistemas de grandes marcas."

3. Britos José, D. (2010).

"Se abordado la detección de intrusiones con dos herramientas novedosas, las redes neuronales y las colonias de hormigas. En primer lugar, se comprueba que la red neuronal puede entrenarse fácilmente para distinguir entre condiciones normales y en condiciones de ataque de la red. Se obtuvo un error de aprendizaje de 0,56 % y un error de generalización de 1,97 %, utilizando una configuración sencilla de la red neuronal (configuración "back-propagation" con sólo dos neuronas en la capa oculta). Este resultado se ha logrado por el uso del módulo procesador estadístico que colabora en forma eficiente en la detección de intrusiones. Como se puede advertir, para la detección de inundaciones UDP el aporte realizado por los parámetros relacionados con el protocolo IP es pequeño en relación al aporte de los parámetros del protocolo UDP al

momento de llevar a cabo la detección. Por esta razón, se podría omitir la utilización de los parámetros del protocolo IP.

El sistema se podría adaptar para detectar otros tipos de intrusiones, tales como inundaciones TCP-SYN e ICMP (Internet Control Message Protocol, Protocolo Internet de Mensajes de Control). En el caso de inundaciones TCP-SYN, se debería incluir el uso de parámetros relacionados al protocolo TCP mientras que las inundaciones de paquetes ICMP se detectarían a 140 través de los parámetros del protocolo IP."

4. Estrella Quijije, G. D., (2011).

"La seguridad de una red al momento de establecer una conexión con la red de redes, INTERNET, para esto y mediante esta investigación se dará a conocer el uso, las características y ventajas de una tecnología innovadora llamada Honeypot; la cual en base al análisis posterior, permitiría estar más al tanto de las tendencias actuales del modo en que operan los intruso y así aportar como ayuda a mejorar los esquemas de seguridad de la Carrera de Ingeniería en Sistemas Computacionales y Networking de la Universidad de Guayaquil.

Esta tecnología también es considera como una herramienta de investigación y su filosofía se explica con una frase "CONOCE A TU ENEMIGO", ya que al identificarlo y aprender de él y las técnicas que usa, será posible actuar tomando medidas que permitan mitigar en cierto modo las vulnerabilidades existentes en cualquier entorno de red. Por otra parte, la tecnología Honeypot posee una característica en particular, que rompe con todo paradigma establecido en el medio de la Seguridad de Redes, y es que, al contrario de otros métodos de seguridad cuyo objetivo es prevenir los ataques la Honeypot plantea la idea de atraer al atacante con un único fin, aprender de él."

5. Gago Padreny, I. (2015).

   “Se ha desarrollado un sistema de detección capaz de reconocer ataques de denegación de servicio, tanto en redes TCP/IP convencionales, como en la red Tor. Por lo tanto, se ha cumplido el objetivo principal del proyecto. El sistema propuesto combina métodos de elaboración de métricas basados en el grado de incertidumbre del tráfico que fluye a través de la red monitorizada, con la construcción de modelos predictivos capaces de pronosticar su futuro valor. A la hora de tomar decisiones, se ha considerado la diferencia de la última observación, respecto a intervalos de predicción. En el caso de que estos sean superados, se considera un comportamiento impredecible, y por lo tanto anómalo, situación que desencadena la emisión de una alerta.”

2.2. Base Teórica

- **Servidor web**

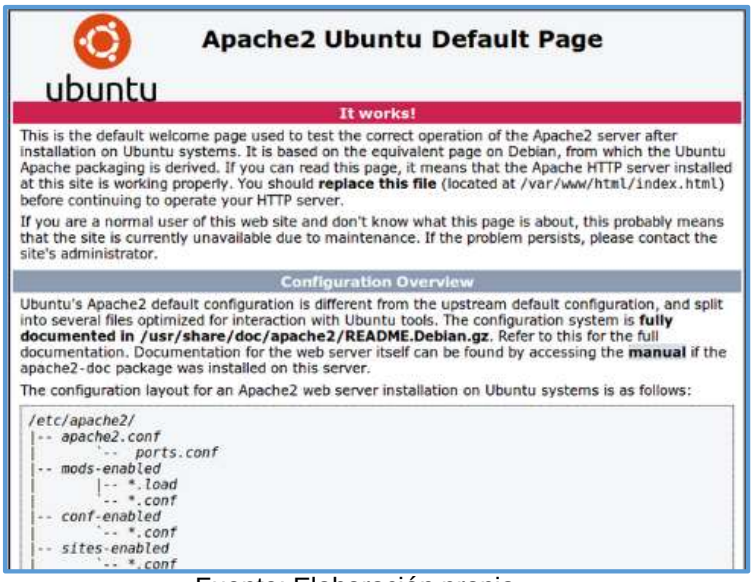
Conforme a Colobran, Arques y Galindho (2008), un servidor web es básicamente lo siguiente: un servidor web sirve su contenido estático a un navegador, carga un archivo, y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP.

Brochard (2006) propone que un servidor web es un ordenador en el que se ejecuta un programa servidor HTTP (Hyper-Test Transfer Protocol), por lo que puede denominarse “servidor HTTP”. Puede utilizarse para publicar un sitio Web en Internet, en una intranet o en una extranet. Un servidor web es un servidor HTTP; es decir, que el ordenador debe tener la capacidad para responder a las solicitudes HTTP de los clientes. Estos clientes son navegadores web.

Según Molina (2007) explica que un servidor web utiliza una aplicación en su sistema para que los usuarios a través de él puedan acceder a

Internet o a una intranet. Las aplicaciones web son populares debido a la practicidad del navegador como cliente ligero.

Figura 7: *Apache instalado correctamente*



Fuente: Elaboración propia.

➢ Servidor Web Apache

Según, The Apache HTTP Server Project. About the Apache HTTP Server Project .Consultado en:
http://httpd.apache.org/ABOUT_APACHE.html

Es un servidor web de código abierto multiplataforma (sistemas Unix, Windows y MacOS, entre otros). Soporta los lenguajes Perl, Python, PHP y Tcl.

Está diseñado para ser un Servidor Web potente y flexible que pueda funcionar en la más amplia gama de plataformas y entornos. Apache se ha adaptado siempre a una gran variedad de entornos a través de su diseño modular. Este diseño permite a los administradores de Sitios Web elegir qué características van a ser incluidas en el servidor seleccionando que módulos se van a cargar, ya sea al compilar o al ejecutar el servidor.

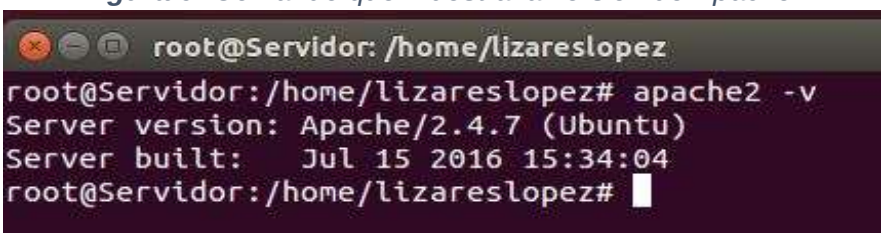
Este servidor Web es el más común y más utilizado en todo el mundo. Además, es gratuito, es una muestra, al igual que el Sistema Operativo Linux, de que el trabajo voluntario y cooperativo dentro de Internet es capaz de producir aplicaciones de calidad profesional difíciles de igualar.

Al ser de código abierto cuenta con una librería pública muy variada y extensa de addons disponibles que se pueden instalar fácilmente. Otras características notables es el Virtual Hosting, que permite que una misma máquina con una instalación de Apache funcione como servidor de varias páginas a la vez.
Apache es el componente de servidor web en la popular plataforma de aplicaciones LAMP, junto a MySQL y los lenguajes de programación PHP/Perl/Python (y ahora también Ruby).

Figura 8: *Comando de instalación de apache en el servidor.*

Fuente: Elaboración propia.

Figura 9: *Comando que muestra la versión de Apache.*



Fuente: Elaboración propia.

➢ Sistema operativo (SO)

Según, Debian. ¿Qué es GNU/Linux? Consultado en https://www.debian.org/releases/stable/armel/ch01s02.html.es

Un sistema operativo consiste en varios programas fundamentales que necesita el ordenador para poder comunicar y recibir instrucciones de los usuarios; tales como leer y escribir datos en el disco duro, cintas, e impresoras; controlar el uso de la memoria; y ejecutar otros programas.

La parte más importante de un sistema operativo es el núcleo. En un sistema GNU/Linux, Linux es el núcleo. El resto del sistema consiste en otros programas, muchos de los cuales fueron escritos por o para el proyecto GNU. Dado que el núcleo de Linux en sí mismo no forma un sistema operativo funcional, preferimos utilizar el término “GNU/Linux” para referirnos a los sistemas que la mayor parte de las personas llaman de manera informal “Linux”.

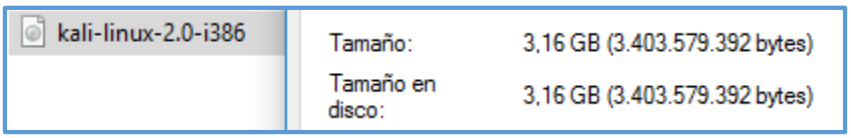
Figura 10: *Sistema Operativo Ubuntu (Servidor)*

Fuente: Elaboración propia.

Existe muchas distribuciones de Linux, una de ellas utilizada en esta investigación es el Kali Linux versión 2.0 una distribución avanzada desarrollada en Debian que agrupa las mejores herramientas para realizar pruebas de penetración y auditoria de seguridad.

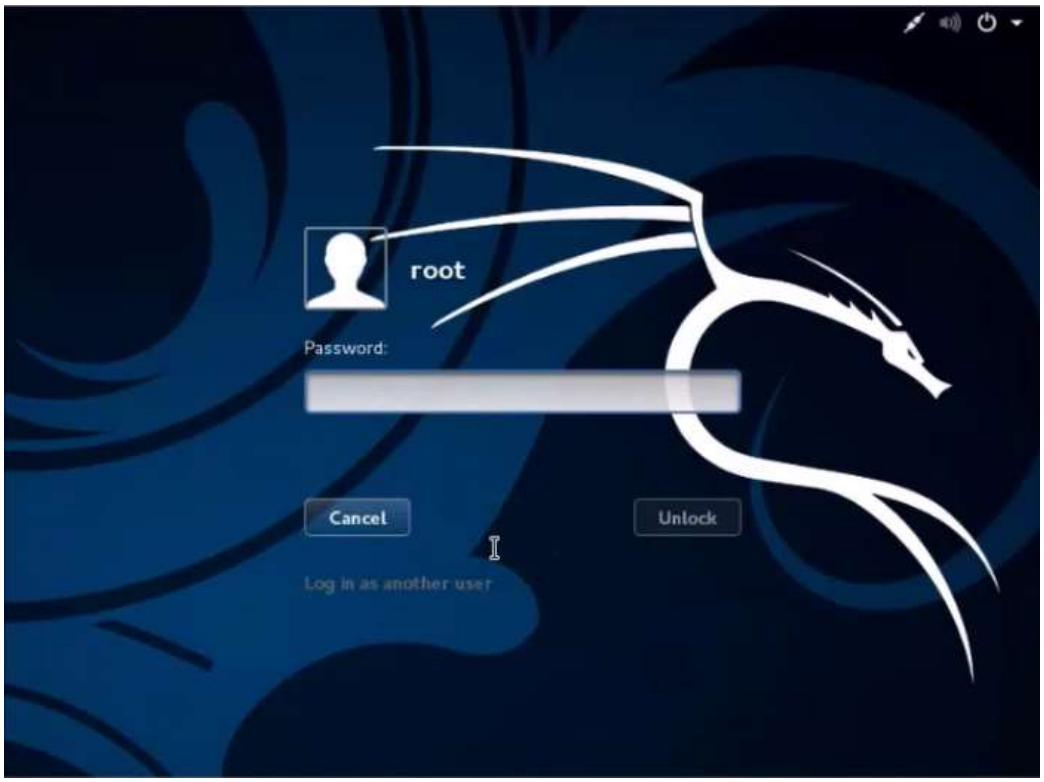
Este sistema operativo es uno de los mejores para llevar a cabo los ataques de denegación de servicio. Por otro parte, existen las imágenes ISO para sistemas de virtualización también tienen su actualización a Kali Linux 2.0 compuesto por un amplio abanico de posibilidades (Kali 2.0 mini, 32 o 64 bits, Virtual Box o VMWare).

Figura 11: *Tamaño de la imagen ISO (Kali Linux 2.0)*



Fuente: Elaboración propia.

Figura 12: *Sistema Operativo Kali Linux (Atacante)*



Fuente: Elaboración propia.

➢ Sistema Operativo Linux(GNU/Linux)

Según, Debian. ¿Qué es GNU/Linux? .Consultado en https://www.debian.org/releases/stable/armel/ch01s02.html.es

Linux está modelado como un sistema operativo tipo Unix. Desde sus comienzos, Linux se diseñó para que fuera un sistema multi tarea y multi usuario.

En 1984 comenzó el desarrollo de lo que más tarde sería GNU/Linux cuando la Free Software Foundation (Fundación de software libre, N. del t.) comenzó a desarrollar un sistema operativo libre de tipo Unix, llamado GNU.

El proyecto GNU ha desarrollado un conjunto de herramientas de software libre para ser utilizados por Unix y sistemas operativos tipo Unix como Linux. Estas herramientas permiten a los usuarios desarrollar tareas que van desde las mundanas (como copiar o eliminar ficheros del sistema) a las arcanas (como escribir y compilar programas o hacer edición sofisticada en una gran variedad de formatos de documento).

➢ Ataques y Vulnerabilidades

Según, La Organización Internacional para la Estandarización (ISO) define la Seguridad de la Información (SI).

La información es un activo esencial para las operaciones de cualquier organización, y por lo tanto necesita ser protegida convenientemente. La seguridad de la información es una disciplina que tiene por objeto asegurar y proteger las tres propiedades fundamentales de la información de los sistemas:

- Confidencialidad: Es la habilidad de un sistema para presentar sus recursos accesibles solo a las partes autorizadas a su uso.

- Integridad: Es la habilidad de un sistema que permite que sólo las partes autorizadas puedan modificarlo y sólo en las formas que son consistentes con las funciones realizadas por el sistema.
- Disponibilidad: Los derechos válidos de acceso a la información nunca deben ser denegados y deben ser satisfechos en tiempo y forma.

Estos paradigmas son conocidos como C. I. A. Algunos autores agregan paradigmas como autenticación, no repudiación, seguridad. Sin embargo, existe un amplio consenso que todos los demás pueden ser derivados de los tres paradigmas básicos.

Es difícil no leer noticias a diario sobre ataques contra redes sociales, ataques DDoS contra servidores y muchos otros golpes llevados a cabo por atacantes informáticos.
Un ataque es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático. También puede ser un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red.

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.

Existe una clasificación de ataques informáticos e intrusos, según la naturaleza de los ataques y estos pueden clasificarse en:

- Pasivos

Se trata de intrusiones en un sistema sin consecuencias para este. Por lo general se hacen para demostrar las vulnerabilidades de un sistema o como retos que se ponen a sí mismo los hackers más experimentados al entrar en sistemas muy protegidos.

- Activos

En esta ocasión la intrusión en el sistema se usa para dañarlo modificando o eliminando archivos. Son los ataques más perjudiciales y con consecuencias más graves.

Según el origen del atacante los ataques pueden ser:

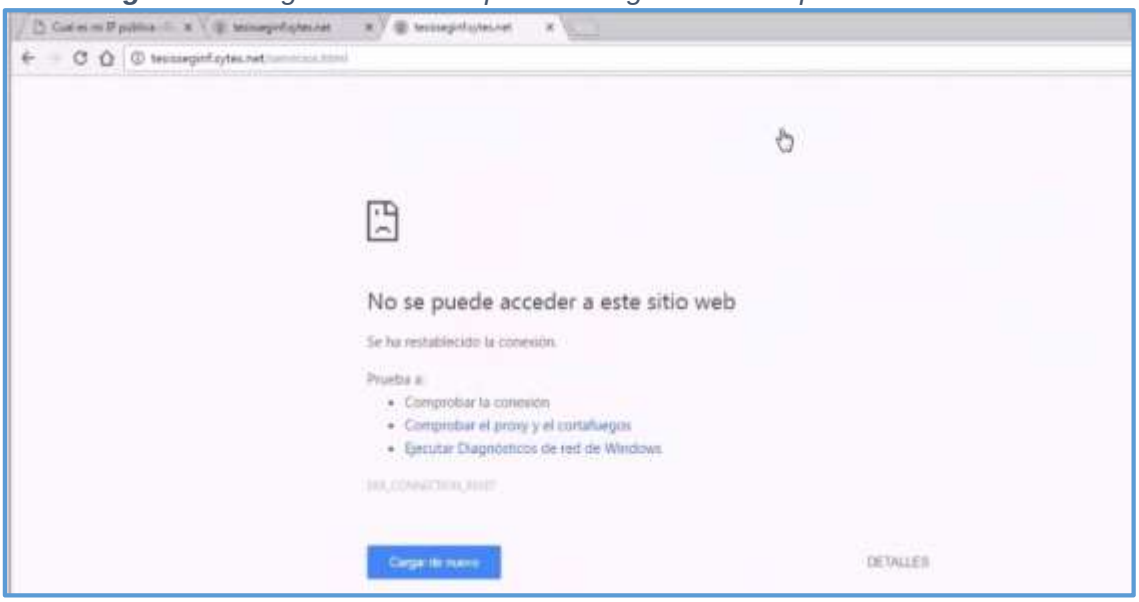
- Internos

El ataque proviene de la propia red. Puede ser realizado por usuarios de la red o por atacantes que suplantan alguna identidad. Son muy peligrosos debido a los privilegios que se tiene sobre el sistema (especialmente si trata de la identidad de un administrador).

- Externos

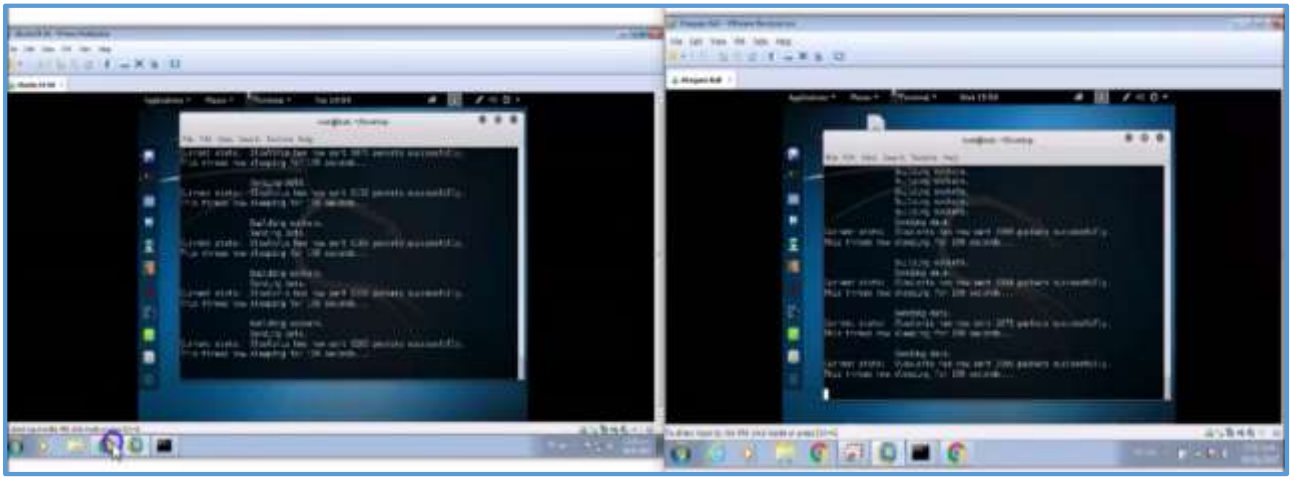
Los ataques provienen del exterior del sistema, en general se hacen a través de internet. Son los ataques más conocidos y lo que se conoce popularmente como hacking o pirateo informático.

Figura 13: *Página web no disponible luego de un ataque externo DDoS.*



Fuente: Elaboración propia.

Figura 14: *Ataques activos y externos a la página web.*



Fuente: Elaboración propia.

- **Ataques de Denegación de Servicio**

Según, Macía Fernández, Gabriel. (2007). *Ataques de Denegación de Servicio a baja tasa contra servidores.* (Tesis Doctoral). Departamento de Teoría de Señal, Telemática y Comunicaciones. Universidad de Granada.

El ataque de denegación de servicio se puede clasificar, dentro de los ataques activos de interrupción. Tienen como objetivo reducir la disponibilidad de un determinado activo en el sistema mediante la realización de un ataque bien a la fuente de información, bien al canal de transmisión o incluso a ambos.

Los ataques de denegación de servicio son diferentes en su objetivo, forma y efecto a la mayoría de ataques que se efectúan contra redes de comunicaciones y sistemas informáticos.
El objetivo de un ataque de denegación de servicio en una red de comunicación es evitar la ejecución de una actividad legitima, tal como la navegación por páginas web, escuchar la radio por Internet, transferir dinero desde la cuenta bancaria o incluso tareas criticas como la comunicación entre un avión y una torre de control.

Existen dos métodos básicos para la realización de un ataque de denegación de servicio: la explotación de una vulnerabilidad descubierta en una maquina objetivo, o el envió de un amplio número de paquetes de apariencia legitima. El primer tipo se denomina usualmente ataque de vulnerabilidad, mientras que el segundo es conocido ataque de inundación.

Los ataques de vulnerabilidad funcionan enviando, a una aplicación que posee una determinada vulnerabilidad, uno o varios paquetes construidos de forma especial. Por otro lado, los ataques de inundación funcionan enviando un numero amplio de mensajes hacia un destino que se convierte en víctima del ataque, de forma que su procesamiento supone un agotamiento de determinados recursos críticos en dicha víctima. Una vez que un recurso está agotado, los clientes legítimos no podrán hacer uso del servicio.

La principal característica de los ataques de inundación consiste en que su fortaleza reside más en el volumen de tráfico que en su contenido

Los ataques que siguen este tipo de estrategias se denominan ataques de denegación de servicio distribuidos (DDoS).

En este punto dela discusión se puede, por tanto, precisar una diferenciación clara entre los ataques de denegación de servicio que se efectúan desde una localización única, es decir, una sola máquina atacante que envía trafico malicioso a un destino, denominado como DoS, y aquellos ataques en los que intervienen numerosas máquinas para atacar a una sola víctima de forma coordinando, para los que se utilizara el llamado DDoS.

➢ Ataques de Denegación de Servicio Distribuido

Según, Cantón Torotosa, G. *Reto de seguridad informática Ataques DDoS y defacemen.*

El concepto de “Distribuido” es concerniente a que estas peticiones son realizadas desde cientos, miles de máquinas infectadas (comúnmente llamadas “zombies”) las cuales son gobernadas a través de “Botnets” de manera coordinada al mismo tiempo, lo cual supone una sumatoria de ancho de banda, uso de memoria y procesamiento, por lo general, ningún servidor podría soportar, terminando en un colapso del servicio atacado por no poder responder cada petición.

Cuando un ataque DDoS son lanzados desde distintos lugares de manera coordinada, se denomina ataque de denegación de servicio distribuido (DDoS).

Para que todos conozcamos un poco mejor de qué formas pueden llegar a atacarnos mediante la denegación de servicios, tenemos algunos de los tipos de ataques conocidos:

- **UDP Flood (Saturación UDP)**

Este tipo de ataque inunda puertos aleatorios de dicho host remoto con numerosos paquetes UDP.

- **ICMP Flood (Saturación por Ping)**

Este tipo de ataque puede consumir tanto ancho de banda saliente y entrante.

- **Service Port Flood (Ataque sobre Puertos de Servicio)**

Las peticiones irán dirigidas hacia los puertos estándar en los que se conoce que habrá más volumen de tráfico

- **HTTP Flood (Saturación HTTP)**

Se hace uso de peticiones GET o POST en apariencia válidas para atacar servidores o aplicaciones web.

- **SYN Flood**

La secuencia de conexión de tres pasos del protocolo SYN. Saturando así el tráfico saliente y entrante del host.

- **Slowloris**

Envía únicamente las cabeceras de las peticiones (HTTP en este caso).

- **Ping of Death (Ping 'de la Muerte')**

Enviar paquetes masivos mediante el protocolo ping.

- **Zero-day DDoS Attack (Ataques 'Día Cero').**

Ataques novedosos o desconocidos que explotan vulnerabilidades de las cuales aún no se han publicado correcciones o parches.

➢ Ataque DDoS Slowloris

Según, Slowloris http dos. Consultado en: http://ha.ckers.org/slowloris/

Es un script programado en perl. Slowloris maneja conexiones abiertas enviando peticiones HTTP parciales. Este continúa enviando cabeceras subsecuentes a intervalos regulares para mantener los sockets. De esta manera los servidores web pueden ser rápidamente atados.

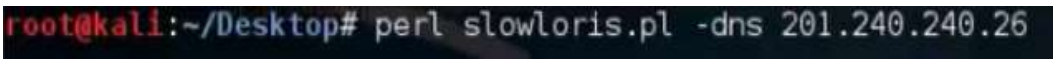
En particular los servidores web que trabajan con hilos tienden a ser vulnerables, por virtud del hecho de que intentan limitar la cantidad de hilos que permiten.

Slowloris debe esperar a que todos los sockets estén disponibles antes de que sean satisfactoriamente consumidos, así es que, si trata de un sitio web con alto tráfico, puede tomar un momento para que el sitio libere sockets.

De esta manera mientras no se es capaz de ver el sitio web desde un punto de vista, otros podrían ser capaces de verlo hasta que todos los sockets sean liberados para ser consumidos por Slowloris. Esto se debe a que otros usuarios del sistema deben finalizar sus peticiones antes de que los sockets estén disponibles para ser consumidos por Slowloris.

Se procede a ejecutar Slowloris. De no ser especificado el puerto, será utilizado por defecto el puerto 80. Luego mediante el siguiente comando empezará a crear los sockets:

Figura 15: *Comando Slowloris utilizado.*



Fuente: Elaboración propia.

Muchos administradores ven en esta herramienta una excelente manera de conocer si el servidor web es vulnerable a dicho ataque.

Figura 16: *Parte del código perl del Slowloris.*

```perl
#!/usr/bin/perl -w
use strict;
use IO::Socket::INET;
use IO::Socket::SSL;
use Getopt::Long;
use Config;

$SIG{'PIPE'} = 'IGNORE';    #Ignore broken pipe errors

print <<EOTEXT;
CCCCCCCCCCOOCCOOOOO888\@8\@8888OOOOCCOOO888888888\@\@\@\@\@\@\@\@\@8\@8\@\@\@\@888OOCooocccc::::
CCCCCCCCCCCCCCCOO888\@888888OOOCCCOOOO888888888888\@88888\@\@\@\@\@\@\@888\@8OOCCoococc:::
CCCCCCCCCCCCCCOO88\@\@888888OOOOOOOOOO8888888O88888888O8O8OOO8888\@88\@\@8OOCOOOCoc::
CCCCoooooooCCCO88\@\@8\@88\@888OOOOOOOO8888888888OOOOOOOOOOCCCCCOOOO888\@8888OOOCc::::
CooCoCoooCCCO8\@88\@88888888OOO888888888888888888OOOOCCCoooooooooCCOOO8888888Cocooc:
ooooooCoCCC88\@88888\@888OO8888888888888888O8O8888OOCCCooooccccccCOOOO88\@888OCoccc
ooooCCOO8O88888888888\@88O8OO88888OO888O8888OOOO88888OCocoocoo::ccooCOO8O888888Cooo
oCCCCCCO8OOOCCCOO88\@88OOOOOO8888O888OOOOOCOO88888O8OOOCooCocc:::coCOOO888888OOCC
oCCCCCOOO88OCooCO88\@8OOOOOO88O8888888OOCCCCoCOOO8888OOOOOOOCoc::::coCOOOO888O88OC
oCCCCOO88OOCCCCOO8\@\@8OOCOOOOO8888888OoocccccoCO8O8OO88OOOOOCc.:ccooCCOOOO8888OO
CCCOOOO88OOCCOOO8\@888OOCCoooCOO8888Ooc::...::coOO88888O888OOo:cocooCCCCOOOOOO88O
CCCOO88888OOCOO8\@\@888OCcc:::cCOO888Oc.....  ....cCOOOOOOOOOOOc.:cooooCCCOOOOOOOOO
OOOOOO88888OOOO8\@8\@8Ooc:.:...cOO8O88c.       .   .coOOO888OOOOCooooccoCOOOOCOOOO
OOOOO888\@8\@8888888Oo:.  .   ...cO888Oc..          :oOOOOOOOOCCoocooCoCoCOOOOOOOO
COOO888\@888888888888Oo:.         .O8888C:   .oCOo.   ...cCCCOOOoooooocccooooooooCCCOO
CCCCOO888888O888888Oo. .o8Oo. .cO88Oo:        :. .:..ccoCCCooCooccooccccoooooCCCC
coooCCO8\@88OO8O888Oo:::... ..   :cO8Oc. . .....   :.   .:ccCoooooccoooocccccooooCCC
:ccooooCO888OOOO8OOc..:...::. .co8\@8Coc::..   ....   ..:cooCooooccccc::::ccooCCooC
.:::coocccoO8OOOOOOC:..::....coCO8\@8OOCCOc:...   ....:ccoooocccc:::::::::coooooooC
....::::ccccoCCOOOOOCc......:oCO8\@8\@88OCCCoccccc::c::.:oCcc:::cccc:..::::coooooo
.......::::::::cCCCCCCoocc:cO888\@8888OOOOCOOOCoocc::.:cocc::cc:::...:::coocccccc
...........::::..:coCCCCCCCO88OOOO8OOOCCooCCCooccc:::ccc::::::.......:ccocccc:co
.............::....:oCCooooooCOOCCOCCCoccococc::::coc:::.......  ...:::cccc:cooo
 ..... ............. .coocoooCCoco:::ccccccc:::ccc::..........  ....:::cc::::coC
   .  . ...    .... ..  .:ccccCooc:..  ::cccc:::c:.. .........  ......::::c:ccccc
  .  .. ... ..    .. ..   ..:...:cooc::cccccc:.....  .........  .....::::ccoocc
      .    .          .. ..::cccc:.::ccoocc:. ........... ..  . ..:::.:::::::ccco
 Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
EOTEXT

my ( $host, $port, $sendhost, $shost, $test, $version, $timeout, $connections );
my ( $cache, $httpready, $method, $ssl, $rand, $tcpto );
my $result = GetOptions(
```

Fuente: Elaboración propia.

➢ Sistema de detección de Intrusos (IDS)

Según, Mira Alfaro, Emilio J. *Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia.* Facultad de Ingeniería Informática. Universidad de Valencia.

Un Sistema de Detección de Intrusos o IDS (Intrusion Detection System) es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.

Definimos intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

La detección de intrusiones permite a las organizaciones proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información.

Los IDSs han ganado aceptación como una pieza fundamental en la infraestructura de seguridad de la organización.

Hay varias razones para adquirir y usar un IDS: Prevenir problemas al disuadir a individuos hostiles.

- Prevenir problemas al disuadir a individuos hostiles.
- Detectar ataques y otras violaciones de la seguridad que no son prevenidas por otras medidas de protección.

Clasificación de los IDSs

Existen varias formas de clasificar los IDSs:

- **IDSs basados en red (NIDS):**
  La mayor parte de los sistemas de detección de intrusos están basados en red. Estos IDSs detectan ataques capturando y analizando paquetes de la red. Escuchando en un segmento, un NIDS puede monitorizar el tráfico que afecta a múltiples hosts que están conectados a ese segmento de red, protegiendo así a estos hosts.

- **IDSs basados en host (HIDS):**

  Los HIDS fueron el primer tipo de IDSs desarrollados e implementados. Operan sobre la información recogida desde dentro de una computadora, como pueda ser los ficheros de auditoría del sistema operativo. Esto permite que el IDS analice las actividades que se producen con una gran precisión, determinando exactamente qué procesos y usuarios están involucrados en un ataque particular dentro del sistema operativo.

A diferencia de los NIDSs, los HIDSs pueden ver el resultado de un intento de ataque, al igual que pueden acceder directamente y monitorizar los ficheros de datos y procesos del sistema atacado.

➢ Módulos Apache

Según, The Apache HTTP Server Project. Apache httpd Modules. Consultado en http://httpd.apache.org/modules/

La arquitectura del servidor Web Apache es modular. Es una manera de agrupar y modularizar ciertos funcionamientos para el servidor, existen una gran cantidad de módulos para utilizarse con Apache.

Una de las principales razones de emplear módulos en Apache, es que no toda instalación requiere de las mismas funcionalidades, por lo tanto, si fueran incluidas todas las funcionalidades posibles en una versión única de Apache, esto lo haría sumamente pesado en cuanto a requerimientos de Memoria RAM y espacio en Disco Duro, por esto se opta por modularizar e incluir solo lo necesario.

El servidor consta de una sección core y diversos módulos que aportan mucha de la funcionalidad que podría considerarse básica para un servidor web.

- **Módulo QoS (mod_qos)**

Según, The Apache HTTP Server Project. Apache httpd Modules. Consultado en http://httpd.apache.org/modules/

Módulo de Calidad de servicio (Quality of Service), es un módulo del servidor HTTP Apache que permite la implementación de mecanismos de control que pueden proporcionar prioridades diferentes a distintas solicitudes.

Podría considerarse el heredero de mod_evasive, el cual estaba diseñado específicamente para protegernos de ataques de denegación de servicio (DoS, Denial of Service). El problema de mod_evasive es que en estos momentos sólo está disponible para la ya vieja rama 1.3 y 2.0 de Apache.

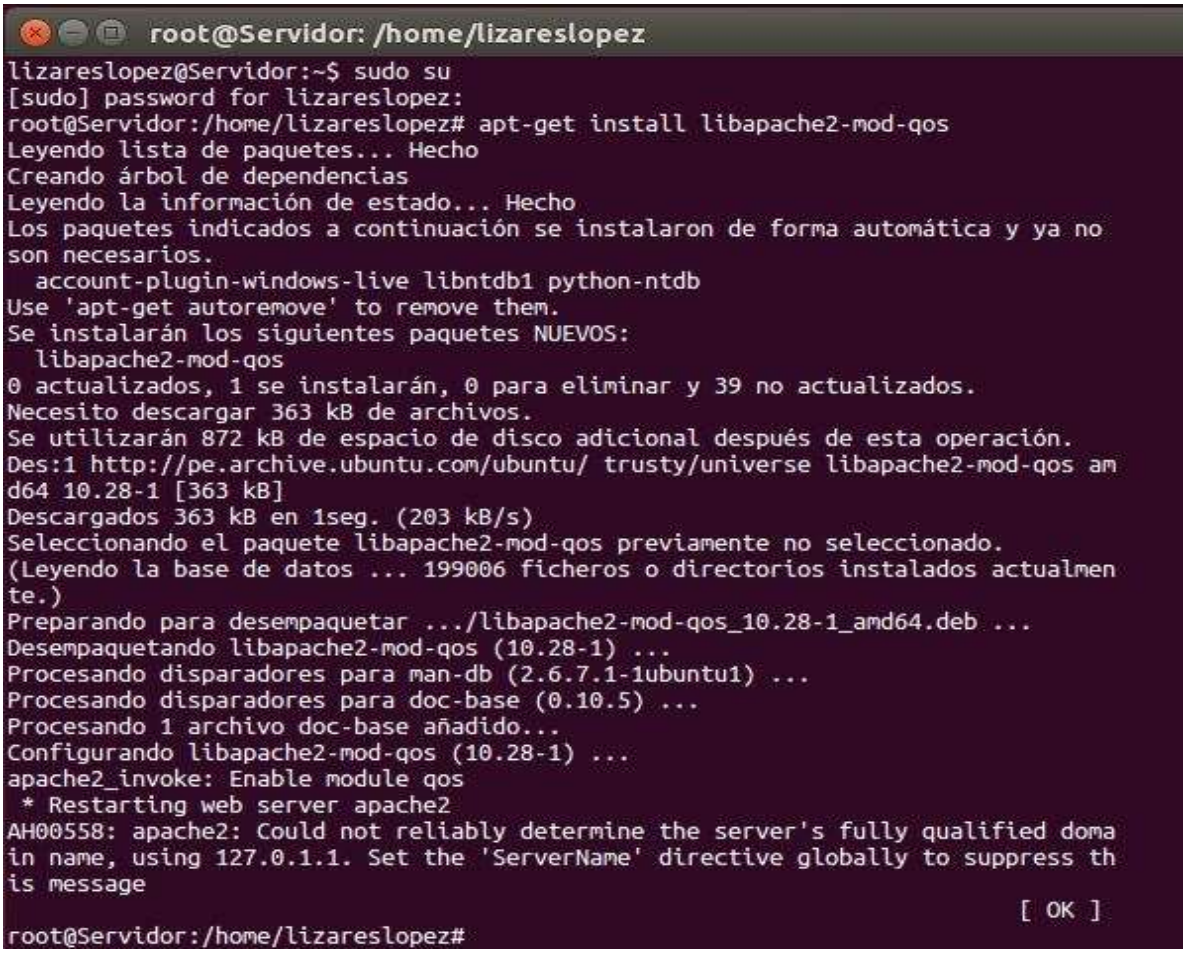
Hoy en día las ramas estables son 2.2 y 2.4, así que se ha quedado un poco vetusto.

Además, mod_qos ofrece algo más que protección frente a ataques de denegación de servicio:

- Ajuste dinámico del ancho de banda dedicado a cada conexión.
- Límite del número de conexiones recurrentes a determinadas URLs. A su vez, también puede ajustar un límite de conexiones por IP.
- Ajuste dinámico de Keep Alive en las conexiones.
- Análisis de cabeceras HTTP para evitar operaciones no autorizadas.

El módulo QoS previene los ataques DoS/DDoS evitando así la sobrecarga de peticiones en el servidor y la caída de los servicios.

Figura 17: *Instalación del módulo QoS en la terminal del servidor web apache.*



Fuente: Elaboración propia.

➢ Pruebas de ataques a servidores Web

Según Revista Inge Cuc, Vol. 9, N° 2, diciembre, 2013

Inicialmente se realizaron instalaciones del Servidor Web Apache en los sistemas operativos GNU/Linux y Windows Server, usando configuraciones por defecto, con el fin de estudiar diferentes formas de instalación e identificar vulnerabilidades derivadas de este proceso. Posteriormente se realizaron pruebas de penetración mediante Nikto mediante el cual se obtuvieron resultados similares en los dos sistemas operativos, en los que la vulnerabilidad más relevante detectada en este proceso fue la utilización de una versión desactualizada del Servidor Web.

Posteriormente se procedió a instalar una versión actualizada del sistema, obtenida del sitio Web de Apache, y se realizó nuevamente una prueba de penetración, en la que las vulnerabilidades más relevantes fueron la aceptación de la línea de encabezado ETag para validar contenido almacenado en caché y aceptación de solicitudes HTTP con el método Trace. Se debe destacar que lo más importante al realizar estos análisis de vulnerabilidades es que luego de la realización de una misma prueba puede dar resultados diferentes si son realizadas en diferentes tiempos.

Luego de obtener las vulnerabilidades se estudió cada una de ellas, se establecieron las contramedidas correspondientes para cada caso y se aplicaron a la configuración del Servidor Web Apache en los escenarios virtuales. Es importante resaltar que al intentar contrarrestar una vulnerabilidad (por ejemplo, la versión desactualizada del Servidor Web Apache) pueden surgir nuevas vulnerabilidades, lo que hace necesario repetir el procedimiento para comprobar la efectividad de las contramedidas aplicadas e identificar nuevas vulnerabilidades derivadas del proceso realizado.

Además de los hallazgos realizados por las herramientas tipo escáner aplicadas al Servidor Web Apache existe un conjunto de acciones recomendables para mejorar las condiciones de seguridad relacionadas con la configuración del Servidor Web Apache.

Entre las recomendaciones o buenas prácticas más relevantes están las siguientes: tener un conocimiento completo de todos y cada uno de los elementos del archivo de configuración de Apache (estructura, parámetros y valores), ya que incluir elementos desconocidos o cargar módulos innecesarios puede comprometer la seguridad del sistema; realizar una gestión de usuarios de manera que se garantice el monitoreo constante del ciclo de vida de los usuarios del sistema; esto incluye eliminar cuentas de usuario innecesarias para la prestación del servicio y analizar el alcance de permisos y privilegios de cada usuario

del sistema; verificar constantemente la existencia de archivos en el sistema con permisos de ejecución y monitorear el listado de tareas programadas para evitar la ejecución de acciones no previstas por el administrador del sistema; configurar la huella identificativa del Servidor Web con la mínima información necesaria e incluso, dependiendo de la necesidad, utilizar esta huella identificativa como un elemento distractor para posibles atacantes, cambiándola para indicar un tipo de Servidor Web diferente; y una recomendación final: desplegar los servicios correspondientes al Servidor Web en ambientes operativos exclusivos con el ánimo de evitar vulnerabilidades expuestas por otros servicios prestados en el mismo sistema.

La aplicación de las recomendaciones o buenas prácticas mencionadas, junto con la realización de análisis de vulnerabilidades, no son suficientes para fortalecer las condiciones de seguridad de un Servidor Web Apache. Es conveniente complementar las medidas de seguridad con la instalación y configuración de un firewall de nivel de aplicación. ModSecurity es el firewall de aplicación más comúnmente utilizado para aumentar las capacidades del Servidor Web Apache, debido a que fue desarrollado específicamente para trabajar con este Servidor Web y se instala como módulo externo.

Este firewall proporciona una capa de seguridad adicional y brinda la capacidad de analizar el tráfico de la red mediante un filtro de solicitudes para detectar actividades sospechosas y prevenir el procesamiento de solicitudes HTTP maliciosas. ModSecurity proporciona protección contra diversos ataques que pueden afectar a servidores Web Apache.

Una vez habilitado el filtrado de solicitudes de ModSecurity, toda solicitud HTTP que llega al Servidor Web es capturada y analizada antes de ser procesada. El análisis es realizado con base en un conjunto de reglas; como consecuencia, si una solicitud no cumple con las reglas configuradas, es rechazada.

Las peticiones son normalizadas antes de ser analizadas. La normalización consiste en modificar cuidadosamente la entrada, para hacer un control sobre el conjunto de símbolos utilizados, y de este modo evitar ataques producto de la manipulación del formato de la solicitud como son ataques de inyección de código o ataques de evasión. Como ya se mencionó, ModSecurity necesita de un conjunto de reglas, las cuales pueden ser reglas básicas o avanzadas, sin embargo, cada caso específico debe ser analizado cuidadosamente para evitar la configuración de reglas innecesarias o inconvenientes, debido al impacto en el rendimiento del Servidor Web Apache.

Finalmente, vale la pena mencionar una buena práctica, que consiste en elegir cuidadosamente la ubicación del Servidor Web, especialmente cuando se encuentra expuesto a redes públicas, como es el caso de Internet; es recomendable evitar la ubicación del servidor en esta zona de acceso público. En su lugar, debe ser ubicado detrás de un firewall de frontera que pueda filtrar las solicitudes que van dirigidas al Servidor, exclusivamente hacia los servicios HTTP y HTTPS legítimos según los puertos establecidos en la configuración, usualmente los puertos 80 y 443, respectivamente.

Lo anterior con el fin de evitar ataques sobre otros puertos abiertos o aplicaciones expuestas en el Servidor Web que no hayan sido considerados en el proceso de aseguramiento, siendo esto ajeno a la responsabilidad del administrador del Servidor Web.

2.3. Definiciones de términos

- **PREVENCIÓN Y DETECCIÓN**

Según, Macía Fernández, Gabriel. (2007). *Ataques de Denegación de Servicio a baja tasa contra servidores.* (Tesis Doctoral). Departamento de Teoría de Señal, Telemática y Comunicaciones. Universidad de Granada.

Prevención: Para proporcionar un primer nivel de seguridad, es necesario prevenir los ataques a la seguridad del sistema que debe ser protegido.

Detección: Una vez que las medidas preventivas se han implementado, hay que considerar que un atacante puede evitar dichas medidas. Será necesario, por tanto, disponer de un método que permita detectar las violaciones de la política de seguridad que se produzcan en el sistema.

- **PROTOCOLO HTTP**

Según, W3C. Hypertext Transfer Protocol (HTTP / 1.1): sintaxis de mensajes y enrutamiento https://tools.ietf.org/html/rfc7230.

HTTP está diseñado para su uso como un protocolo de intermediación para la traducción en la comunicación, desde sistemas de información que no son HTTP. Los proxies HTTP y las puertas de enlace pueden proporcionar acceso a alternativas servicios de información mediante la traducción de sus diversos protocolos en un formato de hipertexto que puede ser visto y manipulado por los clientes en el de la misma forma que los servicios HTTP.

- **PROTOCOLO TCP**

Según, Boulevard, Wilson. Protocolo de Control de Transmisión. Consultado en: https://tools.ietf.org/html/rfc793

El Protocolo de Control de Transmisión (TCP) es un protocolo fiable orientado a la conexión de extremo a extremo diseñado para encajar en una jerarquía de capas de protocolos que soporta múltiples redes aplicaciones. El propósito principal de la TCP es proporcionar una conexión fiable, servicio de circuito o conexión lógica entre pares de procesos asegurables. Para proporcionar este servicio en la parte

superior de una Internet menos fiables el sistema de comunicación requiere instalaciones en las siguientes áreas:

- Transferencia de datos básicos
- Confiabilidad
- Control de flujo
- Multiplexación
- Conexiones
- Precedencia y Seguridad

➢ PROTOCOLO DNS

Según, Microsoft TechNet. Sistema de nombres de dominio. Consultado en: https://technet.microsoft.com/es-es/network/bb629410.aspx

El Sistema de nombres de dominio (DNS) es una base de datos distribuida y jerárquica que contiene asignaciones de nombres de dominio de DNS a diferentes tipos de datos, como las direcciones de protocolo de Internet (IP). El sistema DNS le permite usar nombres sencillos como www.microsoft.com, para localizar equipos de forma fácil y otros recursos en redes basadas en TCP/IP. DNS es un estándar del Grupo de trabajo de ingeniería de Internet (IETF).

CAPÍTULO III

III. MARCO METODOLÓGICO

3.1. Tipo de Investigación

3.1.1. De acuerdo al fin que persigue

De acuerdo al fin que persigue la investigación, se realizara el tipo de investigación aplicada, este tipo de investigación se centra en la utilización y en las consecuencias prácticas de los conocimientos. La investigación aplicada busca identificar para hacer o corregir, tomando como criterio los recursos de donde se adquiere la información.

3.1.2. De acuerdo a la metodología para demostrar la hipótesis

El mejor diseño que se adapta a nuestra investigación es el diseño pre experimental, en su modalidad Diseños de pre test- post test con un grupo, esto significa que a un grupo de sujetos se le aplica en primer lugar el pre test, a continuación, el tratamiento y, por último, el post test. Posteriormente se evaluarán los cambios existentes.

3.2. Variables e Indicadores

Las variables a emplear durante la investigación, serán las siguientes:

Variable N° 1: Modulo de seguridad QoS.	
Tipo:	Independiente
Variable N° 2: Prevención y detección de ataques DDoS al servidor web.	
Tipo:	Dependiente

Tabla 1: *Definición de Variables*

A sí mismo, los indicadores que se utilizarán durante la investigación estarán directamente relacionados con los sistemas de detección de intrusos (IDS).
Los indicadores que emplearemos durante el desarrollo de la tesis serán los verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos.

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).

Para cada indicador consideraremos las definiciones y fórmulas expuestas (Echeverri, O., Trujillo, & Marulanda, 2010):

- **VP: Verdaderos Positivos:** Paquetes correctamente detectados. La Tasa de Verdaderos Positivos está determinada por:

Figura 18: *Formula Verdaderos Positivos.*

$$TasaVerdaderosPositivos(TVP) = \frac{\sum_{i=1}^{n} VP_i}{\sum_{i=1}^{n} A_i}$$

Fuente: Elaboración propia

- **FN: Falsos Negativos:** Paquetes que no fueron detectados, determinada por:

Figura 19: *Formula Falsos Negativos.*

$$TasaFalsos\ Negativos(TFN) = \frac{\sum_{i=1}^{n} FN_i}{\sum_{i=1}^{n} A_i}$$

Fuente: Elaboración propia

- **FP: falsos positivos:** Paquetes que el modelo marcó como objetivos detectados, pero realmente no lo son.

Figura 20: *Formula Falsos Positivos.*

$$TasaFalsos\ Positivos\ (TFP) = \frac{\sum_{i=1}^{n} FP_i}{\sum_{i=1}^{n} N_i}$$

Fuente: Elaboración propia

A partir de lo expuesto podemos definir los indicadores de la siguiente manera:

INDICADOR	ECUACIÓN	PREGUNTA
Tasa de Verdaderos Positivos (VP)	[(Número de Ataques detectados) / (Número Total de pruebas)]*100	¿Cuál es el porcentaje de ataques correctamente detectados?
Tasa de Verdaderos Negativos	[(Número de Tráfico Legítimo Detectado como tráfico normal) / (Número Total de pruebas)] *100	¿Cuál es el porcentaje de tráfico legítimo correctamente identificado como tráfico normal?
Tasa de Falsos Positivos	[(Número de tráfico Legítimo Detectado incorrectamente como Ataque) / (Número Total de Pruebas)]*100	¿Cuál es el porcentaje de tráfico legítimo detectado incorrectamente como ataque?
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?

Tabla 2: *Definición de Indicadores.*

3.3. Población y Muestra

POBLACIÓN:

Durante la problemática planteada, la población es infinita, producto de que el número de atacantes puede ir más allá de cien mil, oponiéndose entonces al concepto de Poblaciones Finitas, con lo cual existe un número ilimitado de usuarios que podrían realizar un ataque DDoS, mediante cualquier herramienta aplicable.

MUESTRA:

Al tratarse de una población infinita necesitamos aplicar ciertos criterios que nos ayuden a encontrar el tamaño de la muestra y así posteriormente obtener la información que nos ayude a corroborar nuestra hipótesis.

Dado que buscamos encontrar el tamaño de una muestra para una población infinita, utilizaremos la siguiente formula:

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

Dónde:

N= Tamaño de la muestra
Z= Nivel de confianza al 95%
P= Variabilidad negativa 50
Q=Variabilidad positiva 50
E= Error 0.049

Para resolver la fórmula se requiere de una tabla que nos dará la cantidad del nivel de confianza; es decir si se elige un 95% de confianza, esto será igual a 0.95, se dividirá entre 2 y nos dará un valor de 0.4750 lo que equivale en la tabla a 1.96. Utilizaremos un error del 4.9% que vendría a ser 0.05 y valores de p=q=0.5.

Para realizar las diversas verificaciones respecto a la prevención y detección de los ataques DDoS se determinaron 400 ataques debido

a un nivel de confianza del 95%, con un error del 4.95% y con valores p=q=0.5. Los 400 ataques a su vez se dividirán en 50 ataques de 8 tiempos.

La duración de los ataques que se realizaron fueron menores a 4 horas y menores a 30 minutos, considerando los periodos de 5, 10, 15, 20, 25, 30, 60 y 90 minutos, esto con la finalidad de determinar la efectividad de la protección al servidor mediante diversos tiempos efectivos.

Además, se realizaron 50 ataques para medir el nivel de protección de los módulos de seguridad mod security y mod evasive en comparación a la herramienta de solución planteada en la tesis.

3.4. Estrategia para la demostración de la hipótesis

Para contrastar nuestra hipótesis existen varios diseños, pero dado el contexto de nuestro estudio, el diseño que mejor encaja para proceder a validar nuestra hipótesis es el diseño pre-experimental.

En la descripción de los diseños pre-experimentales, cuasi experimentales y experimentales de grupo, se emplearán una serie de códigos y símbolos, a fin de comprender la mayoría de sus características distintivas. Una X representa la exposición del grupo a una variable - tratamiento, cuyos efectos se han de medir; O hará referencia a la medición u observación del grupo o individuos; las X y O en fila dadas se aplican a las mismas personas.

La dimensión representada de izquierda a derecha indica el orden temporal, las X y O en una fila dada dispuestas en forma vertical señalan la presentación de simultaneidad. En los diseños más completos como los experimentales, el símbolo R indica la asignación al azar de los sujetos a los grupos o tratamientos.

Para Campbell y Stanley (1978) existen tres de estos diseños:

Diseño de estudio de caso con una sola medición: Existe un grupo que es sometido a una variable independiente, existiendo una sola medición posterior (post test) a dicha intervención.

X1----------O1

Diseño pre test - post test de un solo grupo: Se realiza una observación antes de introducir la variable independiente (O1) y otra después de su aplicación (O2). Si la prueba se administrará antes de la introducción de la variable independiente se le denomina pre test y si se administra después que entonces se llama post test.

O1----------X----------O2

Diseño de comparación con un grupo estático: En este diseño se trabaja con dos grupos, uno de ellos es denominado grupo experimental y es el que recibe la variable independiente o tratamiento y otro llamado grupo control el cual no recibe ningún tratamiento.

Para la demostración de nuestra hipótesis usaremos el Diseño pre test - pos test de un solo grupo, debido a que es el que mejor se adapta al tipo de estudio que se realizara. Nuestra primera observación O1 se llevará a cabo sin haber introducido nuestra variable independiente que es la implementación del módulo qos (X), posteriormente se realizara la segunda observación ya con la aplicación de la variable independiente y obtendremos O2. Por ende, obtendremos un pre test y un pos test que serán registrados en fichas para poder más adelante detallar la información obtenida en fuente confiable estadísticamente, basándose en el siguiente diseño:

O1----------X----------O2

3.5. Materiales, herramientas y equipos

3.5.1. Software

Requerimiento	Nombre	Costo
Sistema Operativo	GNU/Linux Ubuntu 14.04 (.ISO)	0.00
Sistema Operativo	Kali Linux 2.0 (.ISO)	0.00
Servidor Web	Apache	0.00
Gestor de Base de datos	MySQL	0.00
Lenguaje de programación	PHP	0.00
Dominio (DNS)	El servicio DNS de No-IP	0.00
Script para DDoS	Slowloris.pl (perl)	0.00
Módulos Apache (mod)	QoS	0.00
Página Web	HTML, Css, Ajax, js., fonts, themes	0.00
Editor de codificación	Notepad++	0.00
Máquina Virtual	VM Virtual Box	0.00
Máquina Virtual	VM Ware	0.00
Otros	Código fuente	0.00

*El costo es 0.00 por que el software es de licencia libre o gratuito.

Tabla 3: *Costo de cada Software utilizado.*

3.5.2. Servicios

Ítem / Servicios	Descripción	Funciones	Cantidad	Costo Unitario (S/.)	Costo Total (S/.)
Internet	Router BHS-RTA (Movistar)	Acceso a Internet Acceso a la página web Acceso a un ip publica	3 meses	30	90
	Router Mitrastar (Movistar)	Acceso a Internet Acceso a la página web Acceso a un ip publica Acceso a la interfaz del router	3 meses	30	90
	Router Arris (Claro)	Acceso a Internet Acceso a la página web Acceso a un ip publica	3 meses	30	90

*Se estima que durante 3 meses se realizaran las pruebas correspondientes, por lo que el servicio de Internet será fundamental para la realización de dicho proceso.

Tabla 4: Servicios utilizados.

3.5.3. Materiales

- **Materiales:** Para realizar el diseño esquematizado de cómo sería los escenarios posibles de nuestro estudio de investigación utilizamos los siguiente:

  - Papel
  - Formatos digitales
  - Lapicero

3.5.4. Equipos

- **Equipos:** Los equipos u ordenadores involucrados en la realización de las pruebas y demostraciones que se llevan a cabo para determinar la fiabilidad de la investigación, son los siguientes:

  - Computadoras de escritorios (PC).
  - Computadoras portátiles (Laptop).
  - Routers

3.6. Técnicas e instrumentos para la recolección de datos

Las técnicas utilizadas para la recolección de datos en esta investigación son las siguientes:

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.

Observación: Es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su

posterior análisis.

La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Es el registro visual de lo ocurre en una situación real, clasificando y consignando los acontecimientos pertinentes de acuerdo con algún esquema previsto y según el problema que se estudia. Previamente a la ejecución de la observación el investigador debe definir los objetivos que persigue, determinar su unidad de observación, las condiciones en que asumirá la observación y las conductas que deberán registrarse.

Observar científicamente significa observar con un objetivo claro, definido y preciso. El investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación

- **Observación Directa y/o Participante:** Cuando el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar. Cuando para obtener los datos el investigador se incluye en el grupo, hecho o fenómeno observado, para conseguir la información.

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

- **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, puede realizarse de varias maneras:

- ❖ Cada individuo observa una parte o aspecto de todo.
- ❖ Todos observan lo mismo para cotejar luego sus datos (esto permite superar las operaciones subjetivas de cada una).
- ❖ Todos asisten, pero algunos realizan otras tareas o aplican otras técnicas.

3.7. Análisis de datos

Mediante una serie de pruebas o procesos, usando herramientas de software y la ayuda de otros equipos que servirán como 'atacantes', se realizaron las siguientes acciones

1. Lograr exponer la vulnerabilidad del servidor web, comprometiéndolo ante situaciones de ataques del tipo DDoS reales y monitorizados.
2. Implementar las herramientas de seguridad contra los ataques.
3. Realizar nuevamente una serie de ataques monitorizados para comprobar el funcionamiento del software instalado.

Una vez realizados los procesos de pruebas finales, verificar que el módulo realice su trabajo, documentar los errores, localizar las causas, repararlas y generar acciones de prevención.

Para el análisis de datos en esta investigación se utiliza la técnica cuantitativa, primero se tendrán en cuenta las variables o indicadores definidos tales como la cantidad de ataques que son prevenidos por el módulo de seguridad, otro variable sería la cantidad de ataques detectados por el servidor, su eficacia se basa en la proporción de ataques reales que son capaces de detectar sin equivocarse. También se debe afrontar los falsos

positivos, que es poder distinguir a los usuarios cuyo acceso son legítimos y no durante un ataque.
Para poder clasificar los datos se considerarán diferentes rangos de tiempos ascendentes para conocer el impacto que tienen los ataques hacia el servidor.

Utilizando las técnicas del análisis documental y la observación para la recolección de datos, por medio de un formato físico y digital diseñado por nosotros para llevar a cabo el análisis de datos y obtener así los resultados que nos lleve a demostrar nuestra hipótesis definida.

CAPÍTULO IV

IV. DESARROLLO DE LA PROPUESTA

4.1. Topología de la propuesta

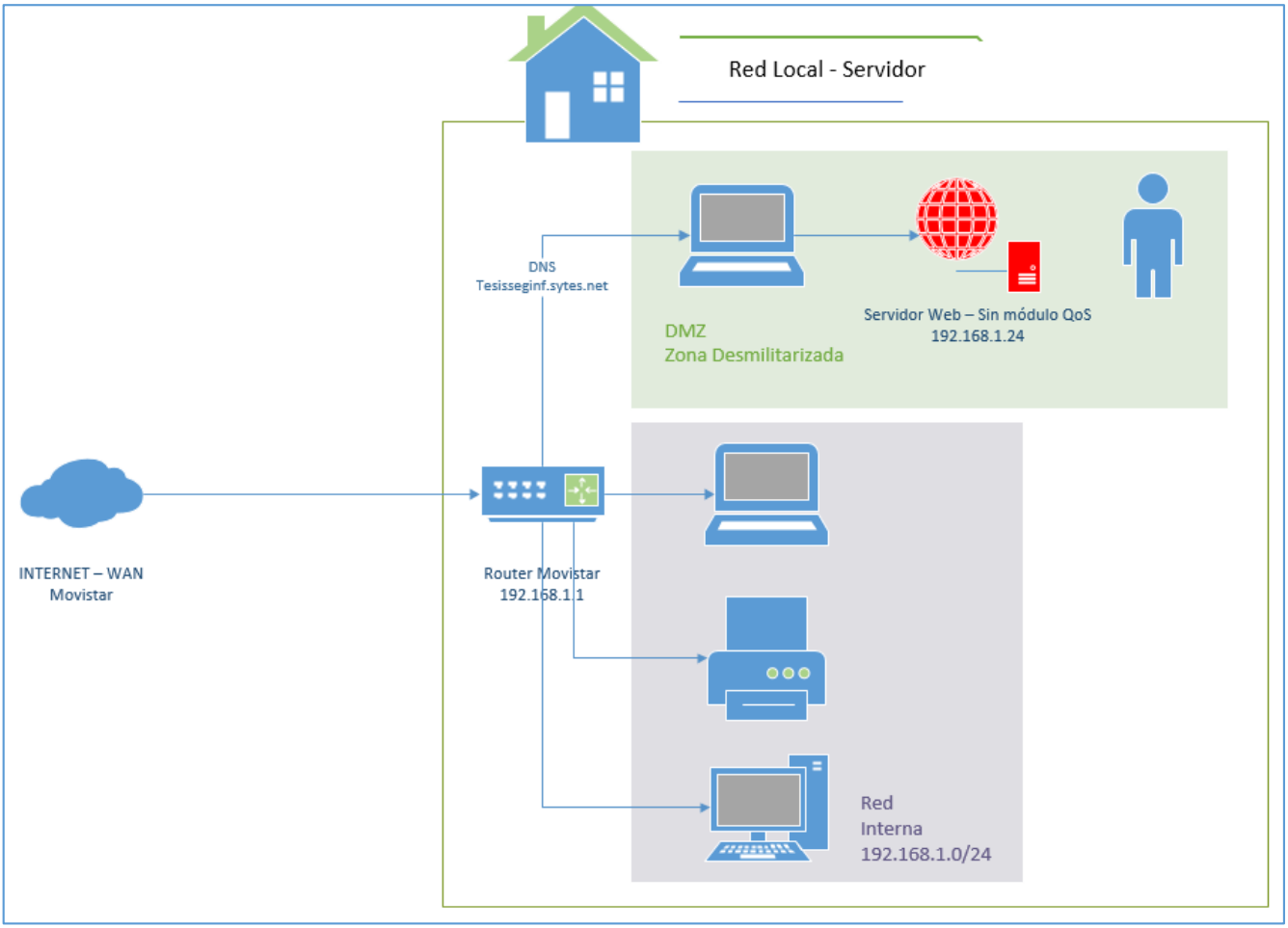
El diseño de la red a trabajar se compone de la siguiente forma:

El servidor web, se encuentra en una Red LAN con conexión a Internet cuyo servicio es público, quiere decir que cualquier usuario o persona puede acceder a la página web desde distintos lugares que se encuentren, la cual está inmerso a múltiples conexiones o accesos durante el tiempo que el servidor este activo y a su vez está propenso a ataques cibernéticos que comúnmente hoy en día se dan.

De acuerdo a lo planificado para el desarrollo de la tesis, se estructuro que física y lógicamente el servidor web se separara de los demás equipos internos dentro de la red local donde se encuentra.

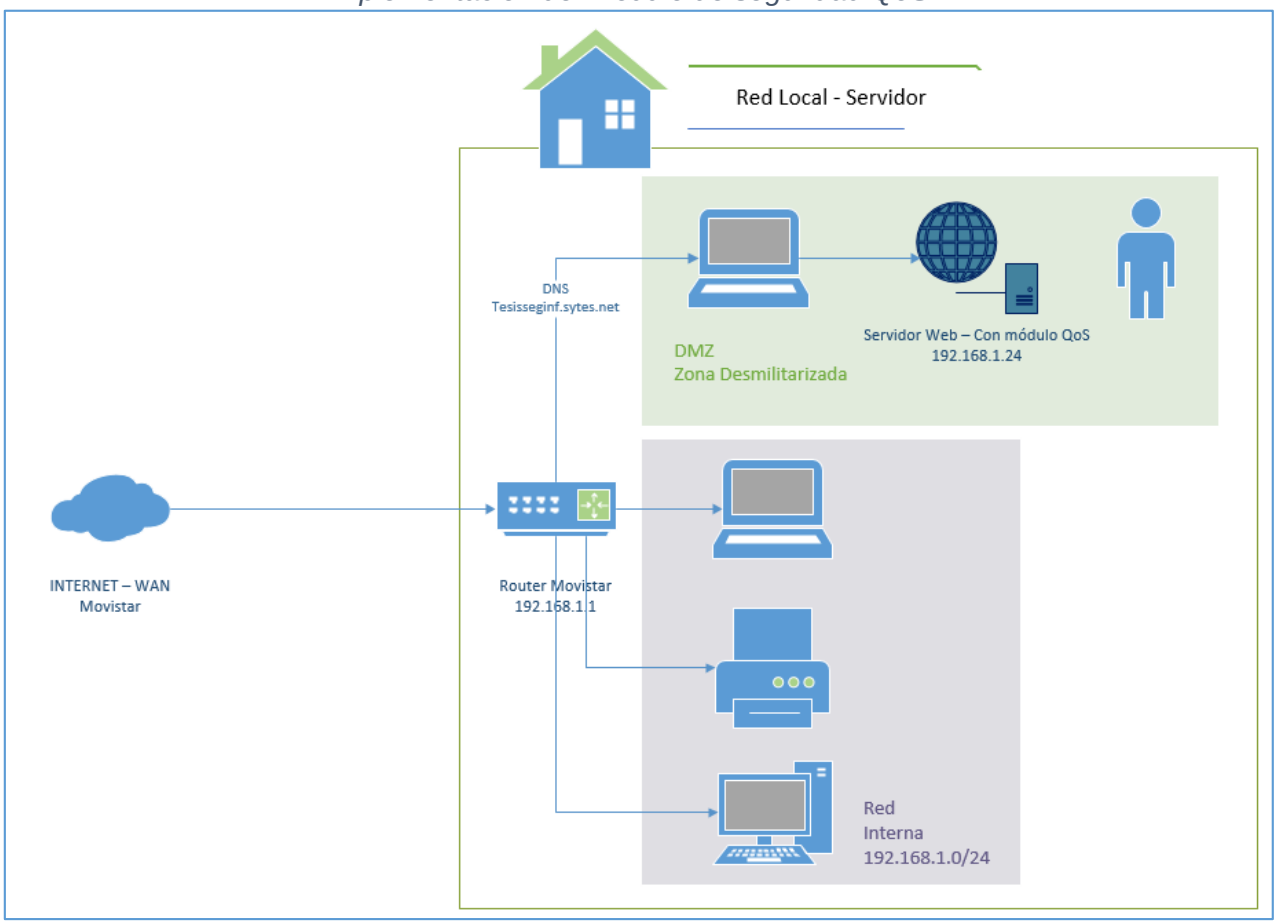
Cuyo diseño es llamado DMZ (Zona Desmilitarizada) el objetivo planteado para este diseño se basa en la seguridad del servidor y la red interna de los demás equipos informáticos.

Figura 21: *La topología por parte de la red local del Servidor está sin la implementación del módulo de seguridad QoS.*



Fuente: Elaboración propia.

Figura 2218: *La topología por parte de la red local del Servidor está con la implementación del módulo de seguridad QoS.*



Fuente: Elaboración propia.

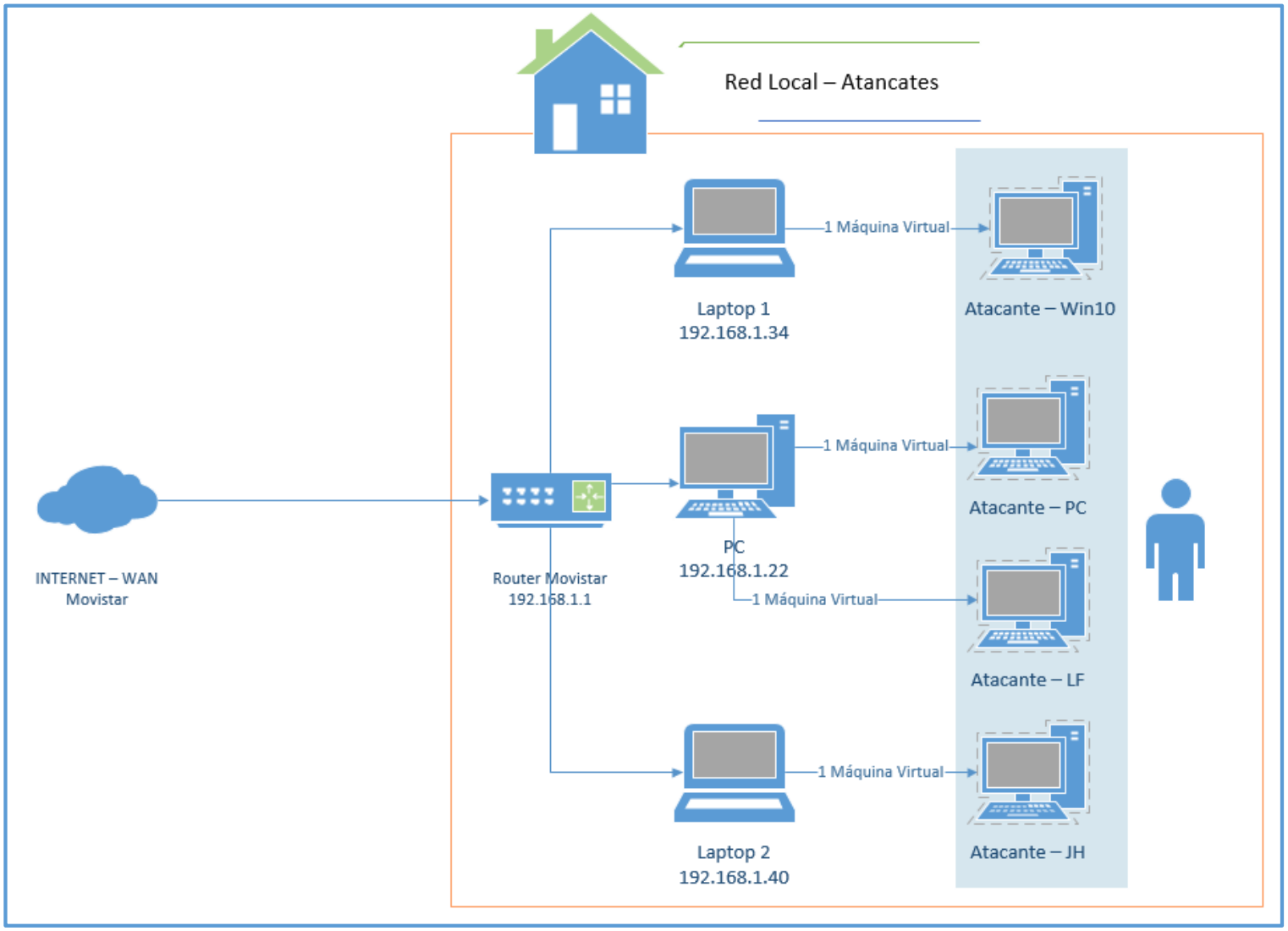
Este diseño a utilizar solo permitirá los ataques externos recibidos fuera de la red local donde se localiza el servidor web. Por lo cual el ataque de la red interna no ha sido considerado en el desarrollo de la tesis.

Si lo consideramos desde el punto empresarial o de cualquier entidad pública o privada que se presente, sus servidores no estarán en peligro dentro de su organización o tal vez exista una mínima posibilidad de riesgo o amenazas que se generen de manera casual o intencionalmente por alguna vulnerabilidad, pero pese a este peligro interno las organizaciones mantienen políticas que impiden que sus trabajadores realicen actividades que no correspondan a lo planificado por lo que la seguridad se centra más en amenazas

externas que afecten la continuidad o productividad del servicio brindado a los clientes o usuarios.

Los equipos atacantes se encuentran también dentro de una Red LAN con conexión a Internet para poder acceder al dominio de la página web del servidor.

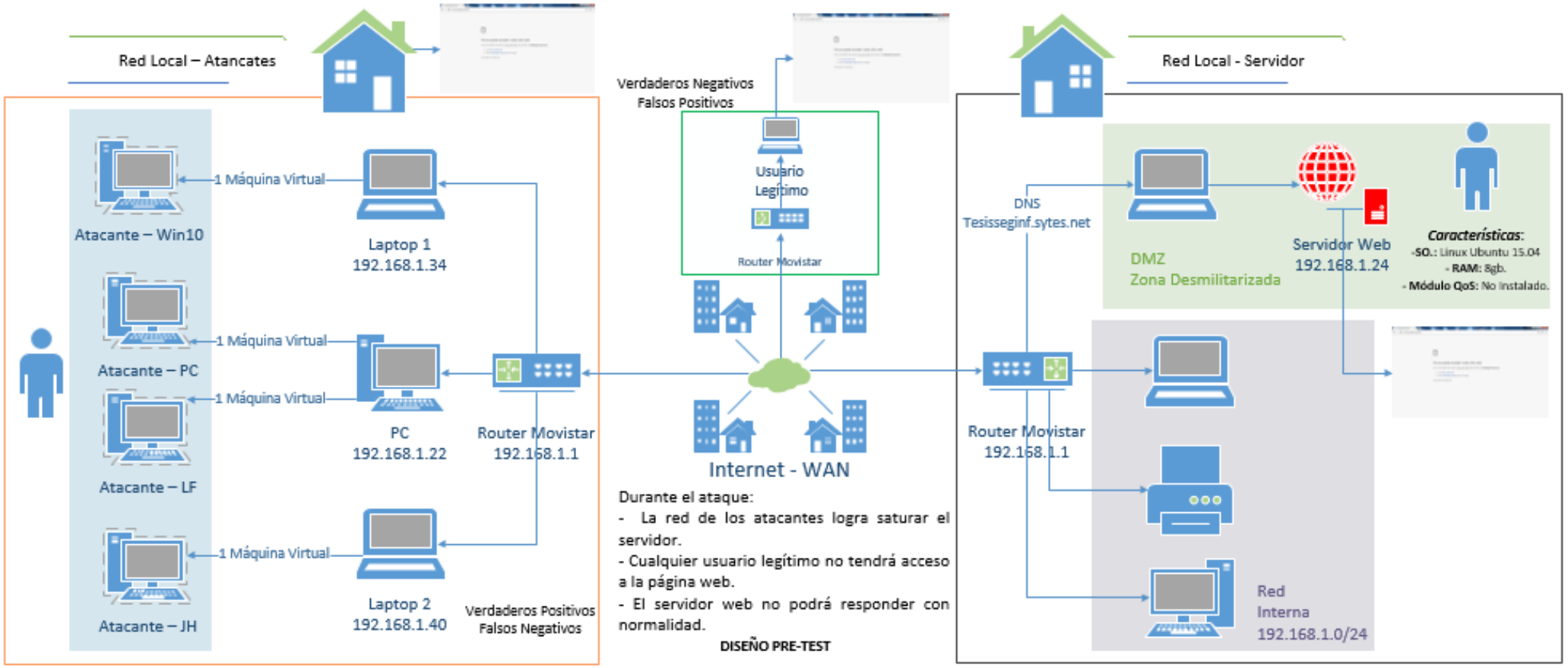
Figura 23: *La topología por parte de la red local de los atacantes.*



Fuente: Elaboración propia.

La topología de la red quedaría de la siguiente manera solo considerando la conexión física que establece el servidor web y la red local de los atacantes, y además de los equipos involucrados para la realización del desarrollo de tesis.

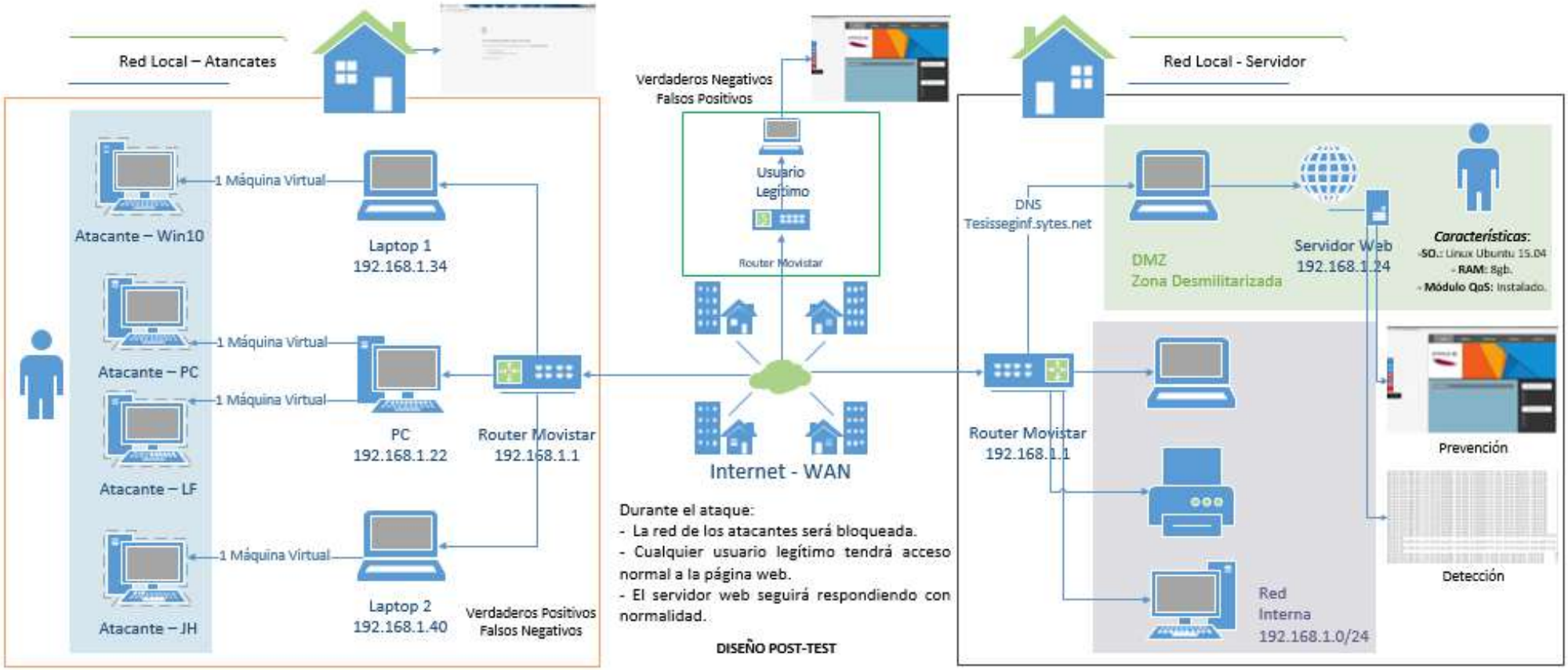
Figura 194: *La topología por parte de la red local del Servidor está sin la implementación del módulo de seguridad QoS.*



Fuente: Elaboración propia

La topología de la red quedaría de la siguiente manera solo considerando la conexión física que establece el servidor web y la red local de los atacantes, y además de los equipos involucrados para la realización del desarrollo de tesis.

Figura 25: *La topología por parte de la red local del Servidor está con la implementación del módulo de seguridad QoS.*



Fuente: Elaboración propia

4.2. Aspectos Técnicos

De acuerdo a la definición de los equipos atacantes dentro del desarrollo de la tesis se componen de 3 equipos físicos de los cuales 2 son equipos portátiles (Laptops) y 1 computadora de escritorio (PC). Cada laptop es un equipo virtualizado que trabaja con una máquina virtual cada uno. En el caso de la PC también es un equipo virtualizado que trabaja en este caso con dos máquinas virtuales, en su conjunto se están considerando 4 equipos virtuales previamente instalados.

Para la asignación de roles se consideró las características propias de cada equipo físico, en la siguiente tabla se especifica los roles de cada atacante.

Figura 206: *Características de los equipos atacantes.*

Equipos Atacantes

Equipo Físico	Nombre de equipo Virtual	Sistema Operativo Físico	Memoria RAM Real	Máquina Virtual	Sistema Operativo Virtual	Memoria RAM Virtual
PC	Atacante - PC	Windows 7	4 GB	Virtual Box	Kali Linux	1 GB
	Atacante - LF	Windows 7	4 GB	Virtual Box	Kali Linux	1 GB
LAPTOP 1	Atacante – Win10	Windows 10	4 GB	VMware	Kali Linux	1 GB
LAPTOP 2	Atacante - JH	Windows 7	2 GB	VMware	Kali Linux	1 GB

Fuente: Elaboración propia.

De acuerdo a la definición del equipo servidor dentro del desarrollo de tesis se compone de un equipo físico el cual es un equipo portátil (Laptop)

Para la asignación de roles se consideró las características propias de cada equipo físico, en la siguiente tabla se especifica los roles de cada atacante.

Figura 27: *Características del servidor web.*

Fuente: Elaboración propia.

4.3. Explicación del Algoritmo Slowloris

De acuerdo al comando a utilizar se especifica lo siguiente:

Parámetros definidos

Perl slowloris.pl **-dns -port -timeout -num -tcpto -test -https -cache -shost –httpready**

-dns: Nombre del host o la Ip pública.
-port: 80 o 443
-timeout: Tiempo de espera para volver a enviar paquetes.
-num: Número de paquetes enviados.
-tcpto: Tiempo de espera de conexiones TCP.
-test: Es una prueba realizada por el propio Slowloris para determinar el timeouts.
- https: Soporte SSL/TLS y enviado hacia el puerto 443.
-cache: Enviando hacia la cache.
-shost: Mostrando sitio web falso.
-httpready: Evita el filtro httpready que almacena en el buffer peticiones completas.

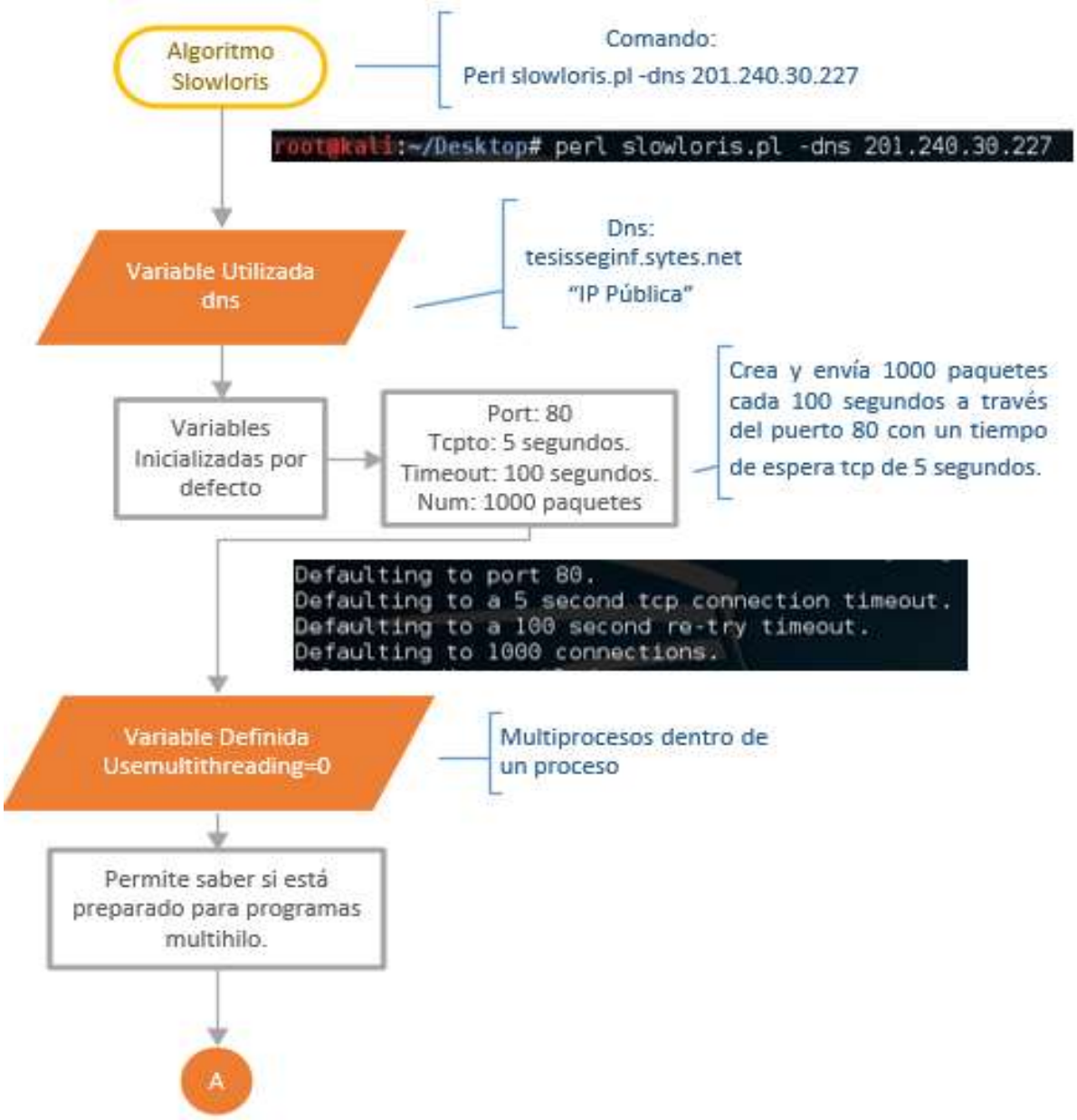
Comando por defecto.

Perl slowloris.pl -**dns** “Host o IP”

- No se especificó el puerto, el timeout, el tcpto ni las conexiones.
- Entonces el algoritmo considera los siguientes valores por defecto: Puerto: 80, tcpto: 5, timeout: 100 y conexiones (num): 1000.
- Lo que quiere decir que enviará el ataque al puerto 80 creando 1000 paquetes cada 100 segundos y con un tiempo de espera TCP de conexión de 5 segundos.

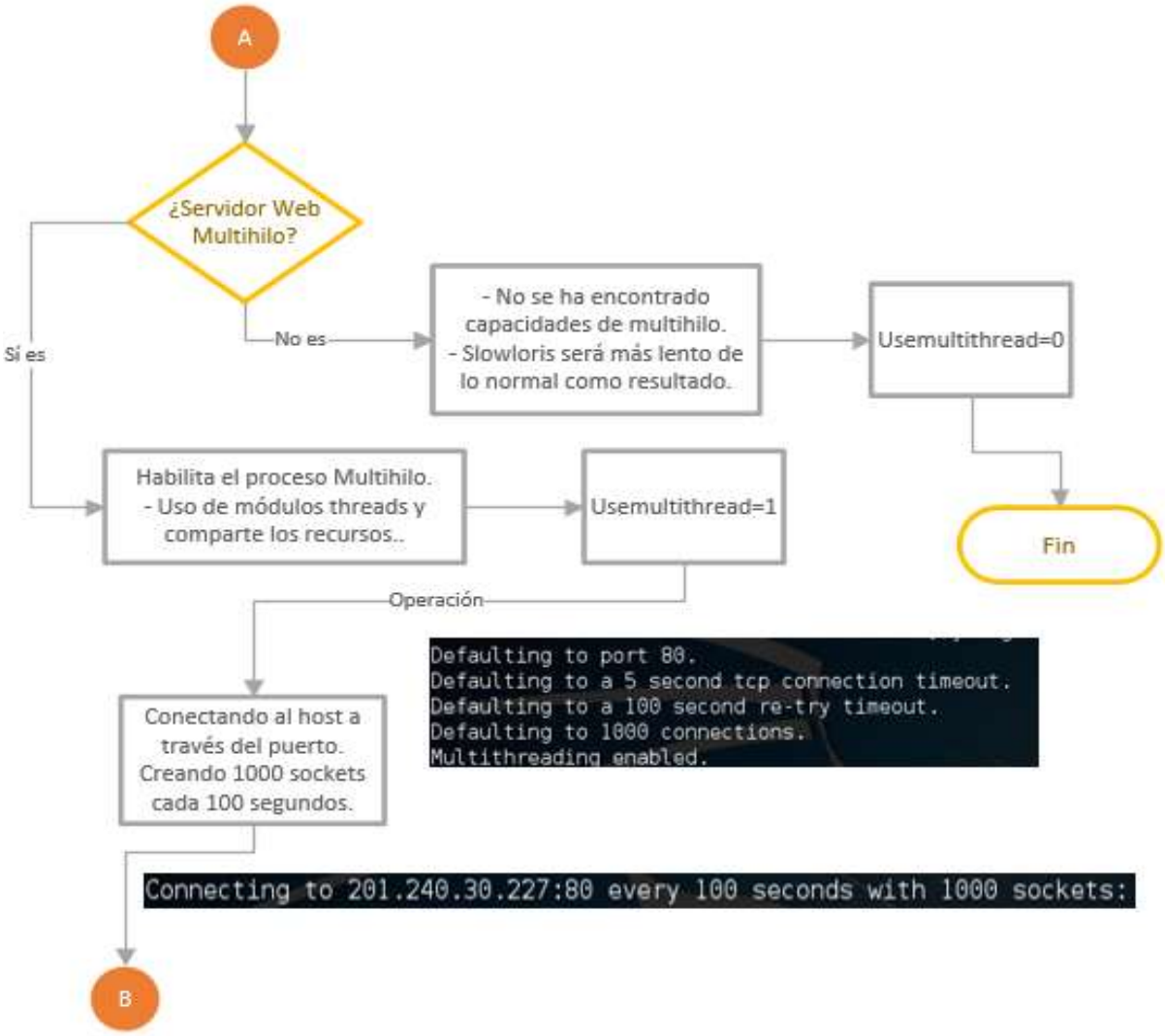
Algoritmo Slowloris modificado (Diagrama de Flujo)

Figura 28: *Diagrama de flujo del algoritmo Slowloris parte 1.*



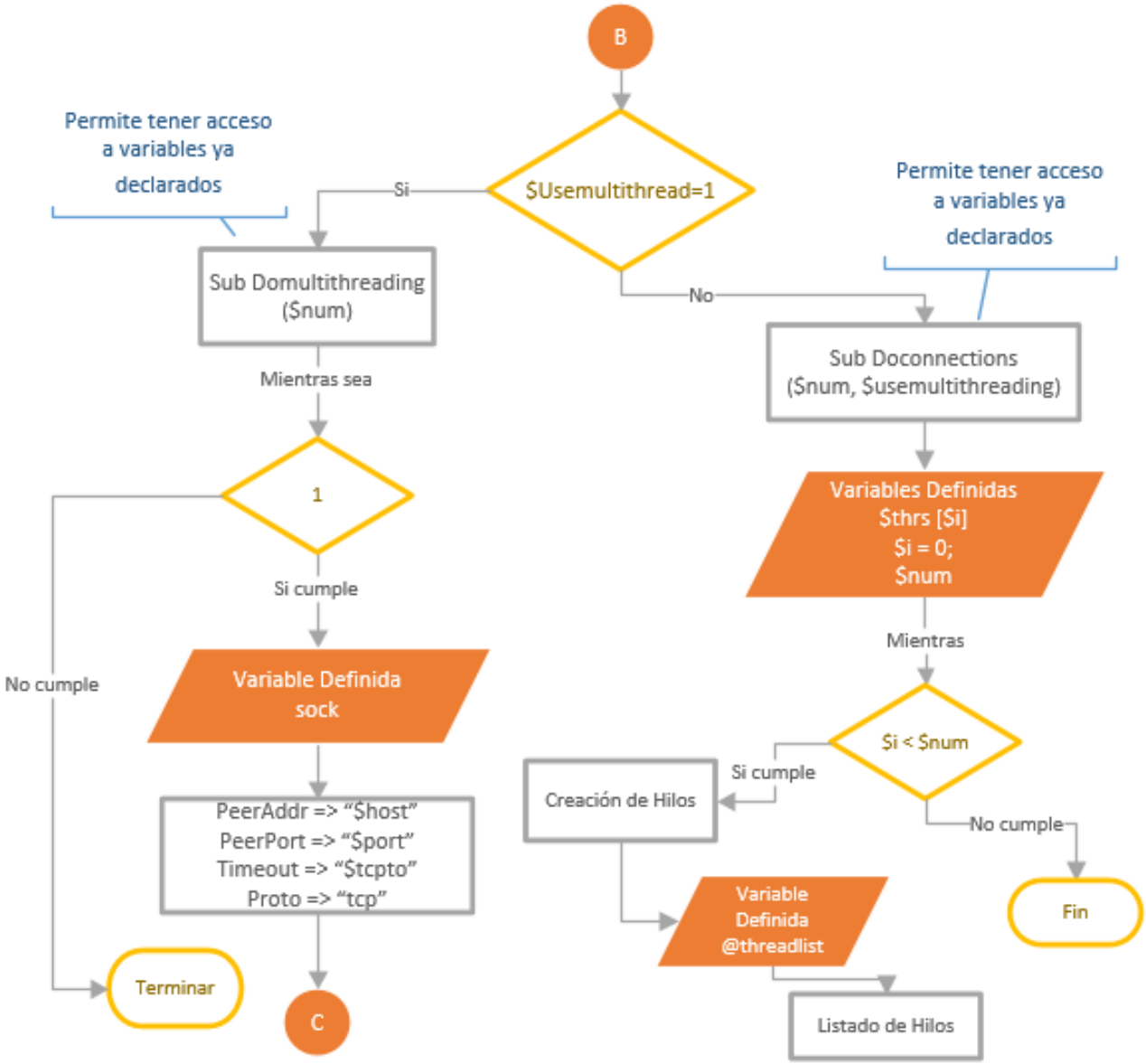
Fuente: Elaboración propia.

Figura 29: *Diagrama de flujo del algoritmo Slowloris parte 2.*



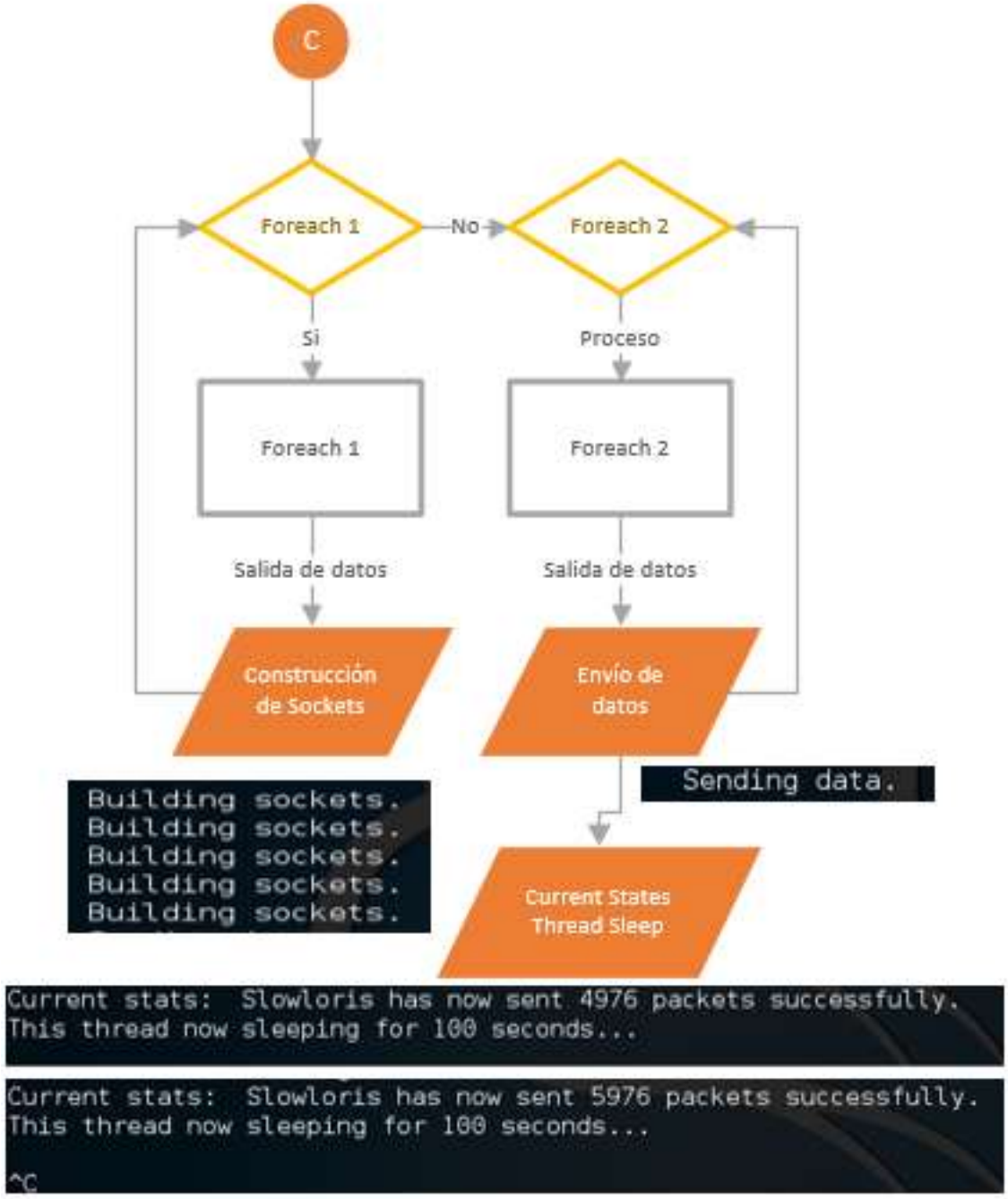
Fuente: Elaboración propia.

Figura 30: *Diagrama de flujo del algoritmo Slowloris parte 3.*



Fuente: Elaboración propia.

Figura 31: *Diagrama de flujo del algoritmo Slowloris parte 4.*



Fuente: Elaboración propia.

Ejecución del script Slowloris (Comando por defecto)

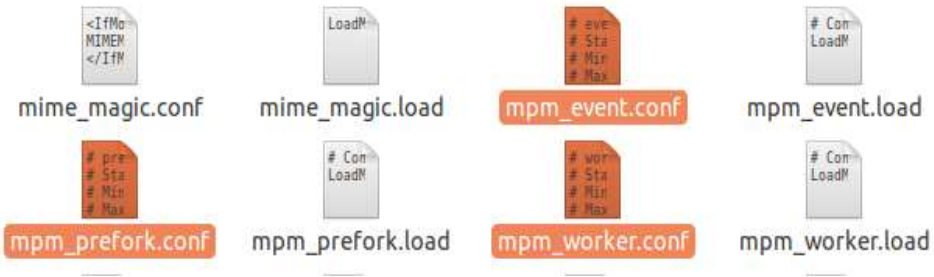
Figura 32: *Ejecución del comando Slowloris por defecto.*

```
root@kali:~/Desktop# perl slowloris.pl -dns 201.240.30.227
```

Fuente: Elaboración propia.

- Luego de enviar el ataque por defecto la variable **$usemultithreading = 0** se inicializa.
- Permite identificar si el servidor web atacado trabaja con multihilos.
- El lenguaje Perl usa los módulos threads para permitir crearlos.
- Como se conoce el servidor web Apache basa su arquitectura en módulos multiprocesos (mpm) con lo cual inicia los procesos y atiende las solicitudes.
- Como la variable **$usemultithreading = 0;** fue ejecutada con éxito cambiará de valor a **$usemultithreading = 1**, el algoritmo continuará el proceso de ataque de lo contrario Slowloris no será una buena alternativa para este caso.
- Los módulos (mpm) que están disponibles dentro del directorio de Apache son los siguientes:

Figura 33: *Módulos disponibles en el directorio de Apache.*



Fuente: Elaboración propia.

Figura 34: *Modulo mpm_worker.conf*

mpm_worker.conf ×

```
# worker MPM
# StartServers: initial number of server processes to start
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadLimit: ThreadsPerChild can be changed to this maximum value during a
#              graceful restart. ThreadLimit can only be changed by stopping
#              and starting Apache.
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestWorkers: maximum number of threads
# MaxConnectionsPerChild: maximum number of requests a server process serves

<IfModule mpm_worker_module>
    StartServers             2
    MinSpareThreads      25
    MaxSpareThreads      75
    ThreadLimit          64
    ThreadsPerChild      25
    MaxRequestWorkers     150
    MaxConnectionsPerChild   0
</IfModule>
```

Fuente: Elaboración propia.

Figura 35*: Módulo mpm_prefork.conf*

mpm_prefork.conf ×

```
# prefork MPM
# StartServers: number of server processes to start
# MinSpareServers: minimum number of server processes which are kept spare
# MaxSpareServers: maximum number of server processes which are kept spare
# MaxRequestWorkers: maximum number of server processes allowed to start
# MaxConnectionsPerChild: maximum number of requests a server process serves

<IfModule mpm_prefork_module>
    StartServers             5
    MinSpareServers       5
    MaxSpareServers      10
    MaxRequestWorkers     150
    MaxConnectionsPerChild   0
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Fuente: Elaboración propia.

Figura 36: *Módulo mpm_event.conf*

mpm_event.conf ×

```
# event MPM
# StartServers: initial number of server processes to start
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestWorkers: maximum number of worker threads
# MaxConnectionsPerChild: maximum number of requests a server process serves
<IfModule mpm_event_module>
    StartServers             2
    MinSpareThreads      25
    MaxSpareThreads      75
    ThreadLimit          64
    ThreadsPerChild      25
    MaxRequestWorkers     150
    MaxConnectionsPerChild   0
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Fuente: Elaboración propia.

Al enviar el ataque se establece los siguientes parámetros por defecto: puerto 80, tcpto de 5, timeout de 100 y 1000 conexiones hacia la Ip pública.

Figura 37: Inicio *del ataque Slowloris.*

Fuente: Elaboración propia.

En condiciones normales, cuando una conexión TCP se cierra, entra en el estado TIME_WAIT ("tiempo de espera"), que por defecto es de 2 minutos. Este lapso de tiempo se emplea para que todos los paquetes que se han quedado "atascados" de alguna manera puedan atravesar igualmente el conjunto de reglas, incluso después de que la conexión se haya cerrado; de esta forma se dispone de una especie de "buffer" de tiempo para que los paquetes que se han quedado parados en algún enrutador congestionado, puedan llegar al cortafuego o al otro extremo de la conexión sin problemas.

Luego se habilita el módulo Multithreading permitiendo compartir variables a través de diferentes subprocesos durante el ataque.

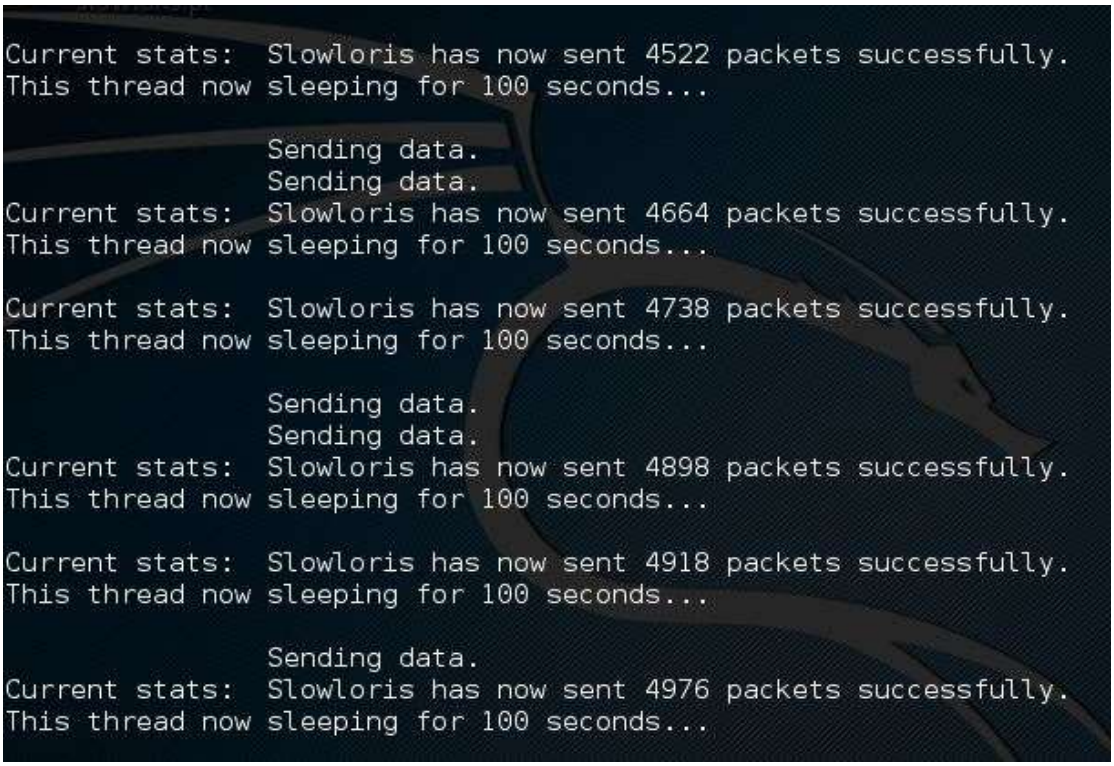
Figura 38: *Ataque Slowloris parte 2.*

Fuente: Elaboración propia.

Se realiza la conexión con el host atacado a través de la ip y el puerto conocido, se van construyendo los sockets por el cual serán enviados los paquetes.

Luego envía 1000 paquetes cada 100 segundos por medio de los 1000 sockets creados anteriormente, en un primer envío la cantidad de paquetes creados es variable por ejemplo en este caso el valor final fue de 4976 paquetes, los valores anteriores son aumentos parciales que se registran hasta llegar a la cantidad final 4976 en un primer momento.

***Figura 39**: Ataque Slowloris parte 3.*



Fuente: Elaboración propia.

Finalmente, luego la variable thead continuará con la creación de hilos y la función speep ($timeout) establecerá un tiempo de espera de 100 segundos para que se vuelva a enviar 1000 paquetes más. Una vez cumplido los 100 segundos, continuará el crecimiento parcial de paquetes hasta lograr completar la cantidad de 5967 y así sucesivamente hasta cancelar el ataque.

***Figura 40**: Fin del ataque Slowloris parte 4.*

Fuente: Elaboración propia.

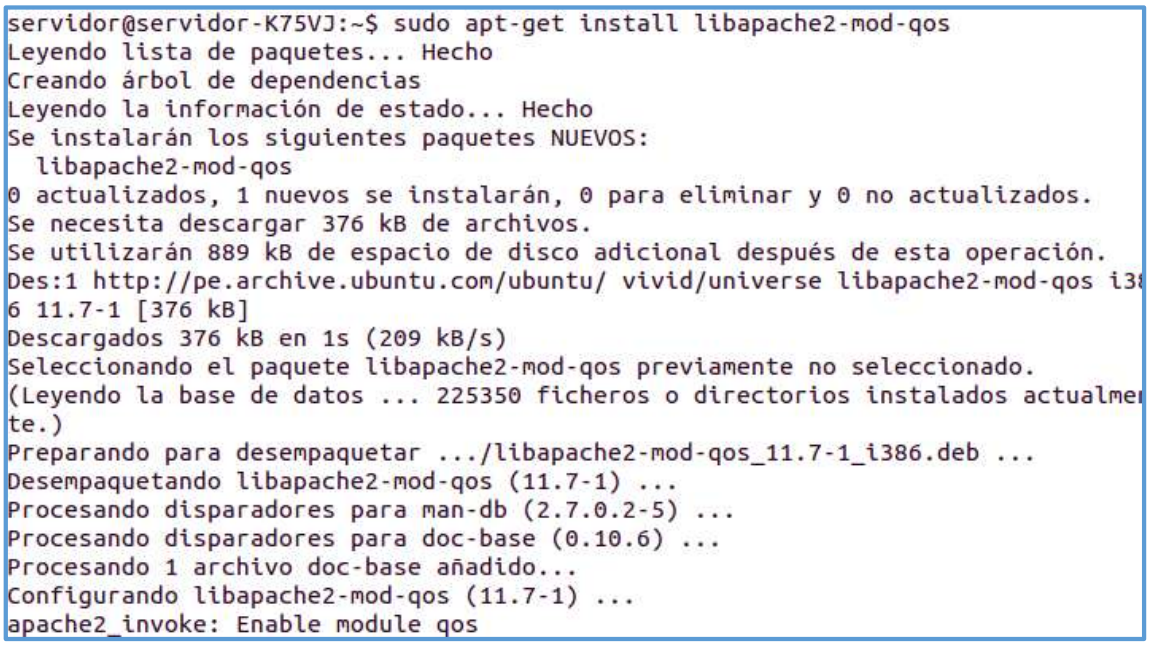
4.4. Implementación del módulo de seguridad mod_qos

Una vez identificado el mecanismo de ataque, en este caso el script Slowloris, procedemos a instalar la herramienta de protección. En primer lugar, instalamos el módulo de seguridad apache mod_qos, para ello ejecutamos el siguiente comando en el terminal de nuestro servidor.

Sudo apt-get install libapache2-mod-qos

Una vez ejecutado el siguiente comando, se instalará correctamente el módulo de seguridad como se muestra a continuación:

***Figura 41**: Instalación del módulo QoS*



Fuente: Elaboración Propia.

Luego de una correcta instalación del módulo de seguridad apache mod_qos debemos editar el archivo de configuración QoS ubicado en

/etc/apache2/mods-available/qos.conf.

Para acceder a la configuración, podemos ejecutar el siguiente comando.

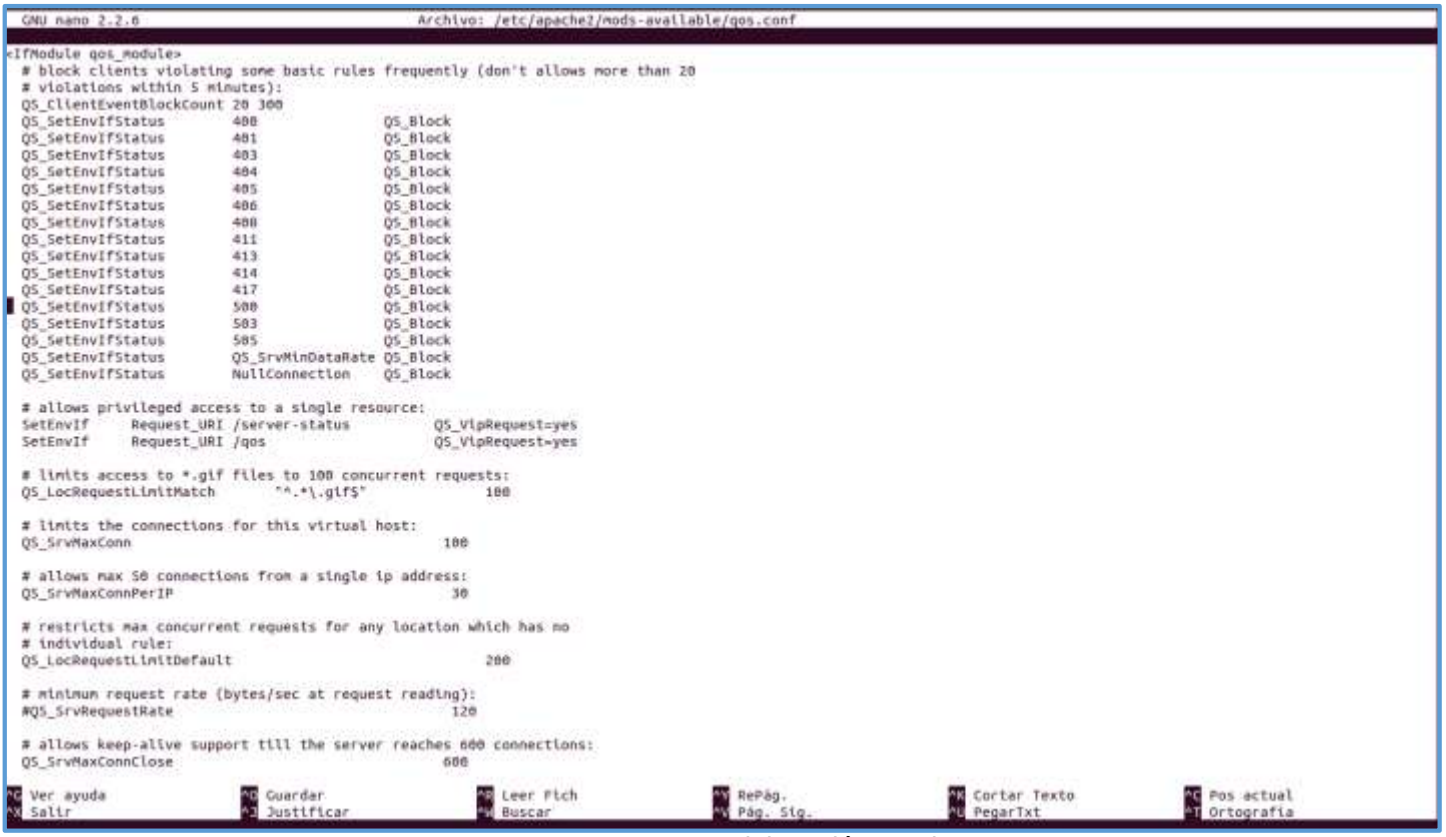
Figura 42: *Comando para acceder a la configuración del módulo QoS.*

```
servidor@servidor-K75VJ:~$ sudo nano /etc/apache2/mods-available/qos.conf
```

Fuente: Elaboración Propia.

Al ejecutarse el comando accedemos a la configuración QoS.

Figura 43: *Configuración del módulo QoS.*



Fuente: Elaboración Propia.

La configuración que se observa no es la que se muestra originalmente al instalar el módulo de seguridad, esta configuración ha sido adaptada de acuerdo a los requerimientos de nuestra investigación de tal manera que podamos obtener los mejores resultados para la protección de nuestro servidor ante ataques DDoS mediante el script Slowloris.

A continuación, explicaremos línea por línea dicha configuración.

- QS_ClientEventBlockCount 20 300

  Define el número máximo de 20 eventos permitidos dentro del tiempo definido de 5 minutos. El IP del cliente se bloquea cuando llega a este contador durante el tiempo especificado (bloqueado en el nivel de conexión: el usuario no siempre obtiene una respuesta de error amigable para el usuario).

- QS_SetEnvIfStatus <code> <env-variable>[=<value>]

  Establece la variable definida en el entorno de solicitud si el código de estado de respuesta HTTP coincide con el código definido. El valor predeterminado es el código de estado, pero puede anularlo por cualquier otro valor. La directiva puede ser utilizada por servidor o por ubicación. Cuando se utiliza la variable especial QS_Block, su valor se establece en "1" por defecto.

- QS_SrvMinDataRate puede utilizarse con el fin de limitar el número permitido de infracciones de reglas.
  .
- NullConnection detecta conexiones que están cerradas, incluso ninguna solicitud HTTP ha sido recibida.

- SetEnvIf Request_URI /server-status QS_VipRequest = yes
  Permite el acceso privilegiado a un único recurso.

- QS_LocRequestLimitMatch "^. * \. Gif $" 100
  Limita el acceso a archivos * .gif a 100 peticiones concurrentes.

- QS_SrvMaxConn <number>
  Define el número máximo de conexiones TCP simultáneas para este servidor (host virtual).
- QS_SrvMaxConnPerIP 30
  Permite un máximo de 30 conexiones desde una sola dirección IP.

- QS_LocRequestLimitDefault 200
  Restringe las solicitudes concurrentes máximas para cualquier ubicación que no tenga regla individual.

- QS_SrvRequestRate 120
  Tasa de petición mínima (bytes / seg en la lectura de la petición).

- QS_SrvMaxConnClose 600
  Permite mantener el soporte hasta que el servidor alcance 600 conexiones.

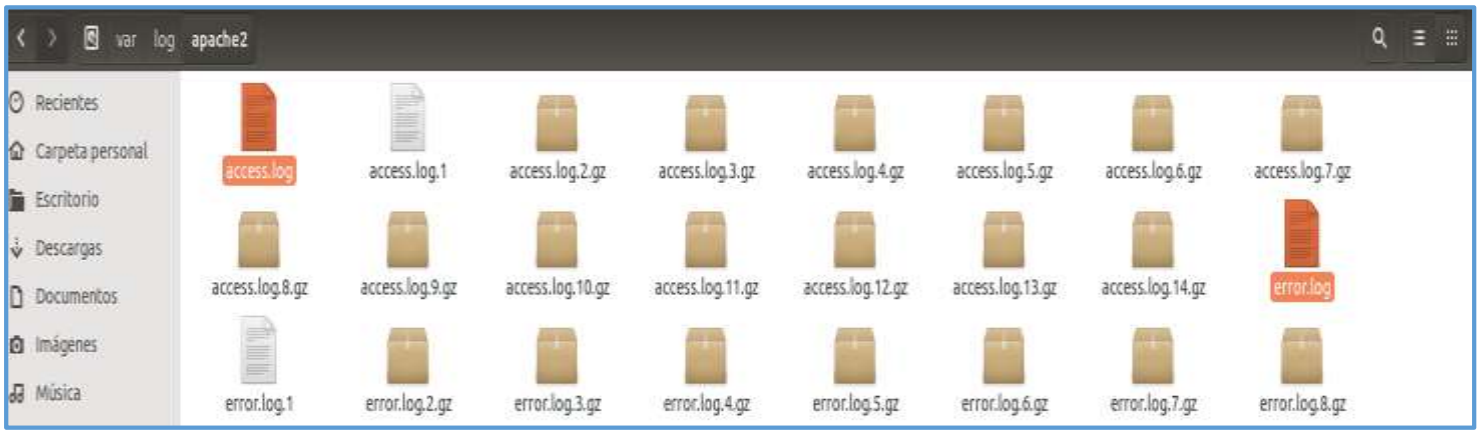
Una vez definida la configuración se procede a reiniciar el servicio de apache con el siguiente comando: service apache2 restart. Para poder realizar o revisar algún cambio posterior debe acceder a /etc/apache2/mods-available/qos.conf.

***Figura 44**: Directorio del módulo QoS*

Fuente: Elaboración Propia.

Además para detectar accesos y ataques podemos acceder a /var/log/apache2 y tanto en el log de Access encontrar todas las ips que acceder a nuestra página web y en el log de error encontramos todas las ips que atacan a nuestro servidor.

Figura 45: *Archivos de registros de acceso y error.*



Fuente: Elaboración Propia.

CAPÍTULO V

V. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

El propósito fundamental de esta investigación fue detectar y prevenir los ataques DDoS en un servidor web mediante la implementación del módulo de seguridad apache mod_qos. Se optó por utilizar el Diseño pre test - pos test de un solo grupo, debido a que es el que mejor se adapta al tipo de estudio realizado.

Empleamos el módulo de seguridad apache mod_qos debido a que fue el que mejor resultados mostro al proteger el servidor web, se cotejaron otros dos módulos de seguridad como el apache mod evasive y el apache modsecurity, ambos no fueron lo suficientemente efectivos para proteger el servidor Web ante un ataque DDoS realizado a través del script Slowloris.

5.1. MÓDULOS DE SEGURIDAD MOD EVASIVE Y MODSECURITY

Al buscar la mejor solución a la problemática planteada, se implementaron ambos módulos de seguridad, ambos por separado, se realizaron 50 ataques de 30 minutos por cada módulo de seguridad.

Se realizaron 50 ejecuciones (ataques) como se menciona a continuación:

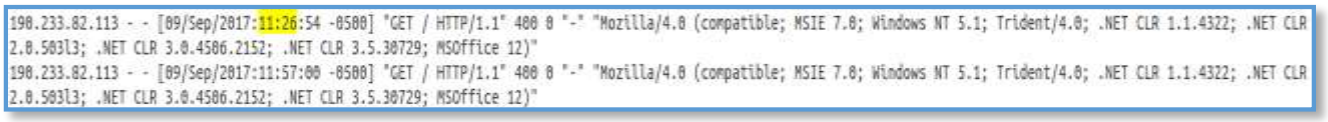
> “Dado que se pretende conseguir un IDS/IPS que funcione en tiempo real y pueda detectar comportamientos anómalos y decidir si bloquea o no una conexión, es necesario reducir la complejidad tanto de la selección de características como de la clasificación (…) A partir de los experimentos realizados con un conjunto reducido de características 8 y un número de 50 ejecuciones” (De la Hoz, 2016, p. 157).

Se obtuvieron los resultados que se muestran a continuación.

5.1.1. MÓDULO DE SEGURIDAD MODSECURITY

El resultado al implementar apache modsecurity fue el siguiente:

Figura 46: *Registro del ataque con módulo Security implementado.*

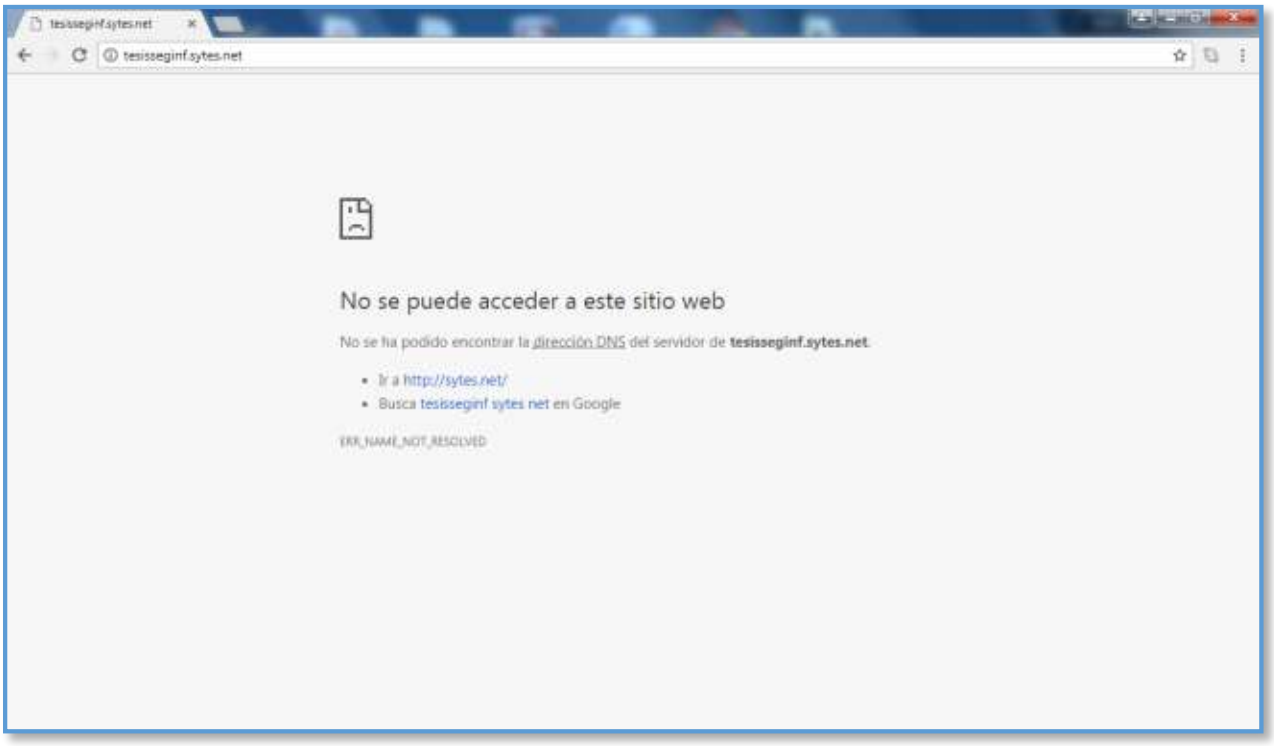


Fuente: Elaboración propia.

Aquí podemos observar que en el log access que contiene el servidor, no ocurre ningún acceso en un lapso de 30 min, desde las 11:27 hasta las 11:57 del día 9 de septiembre del 2017. Durante ese lapso de tiempo se realizó un ataque DDoS al servidor, logrando hacer colapsar la página, por ende la página web no respondió a ninguna solicitud.

Los usuarios no lograron acceder a la página ni una sola vez al iniciarse el ataque DDoS.

Figura 47: *Sin acceso a la página web durante el ataque DDoS con módulo Security implementado.*

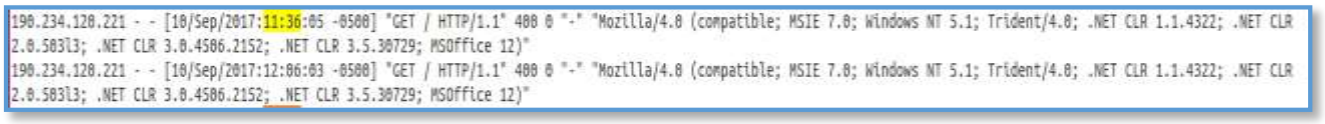


Fuente: Elaboración propia.

5.1.2. MÓDULO DE SEGURIDAD MOD EVASIVE

Una vez comprobado que el módulo de seguridad apache modsecurity no resultaba efectivo para proteger el servidor web de los ataques DDoS, se utilizó el módulo de seguridad apache mod evasive obteniéndose los siguientes resultados:

Figura 48: *Registro del ataque con módulo Evasive implementado.*

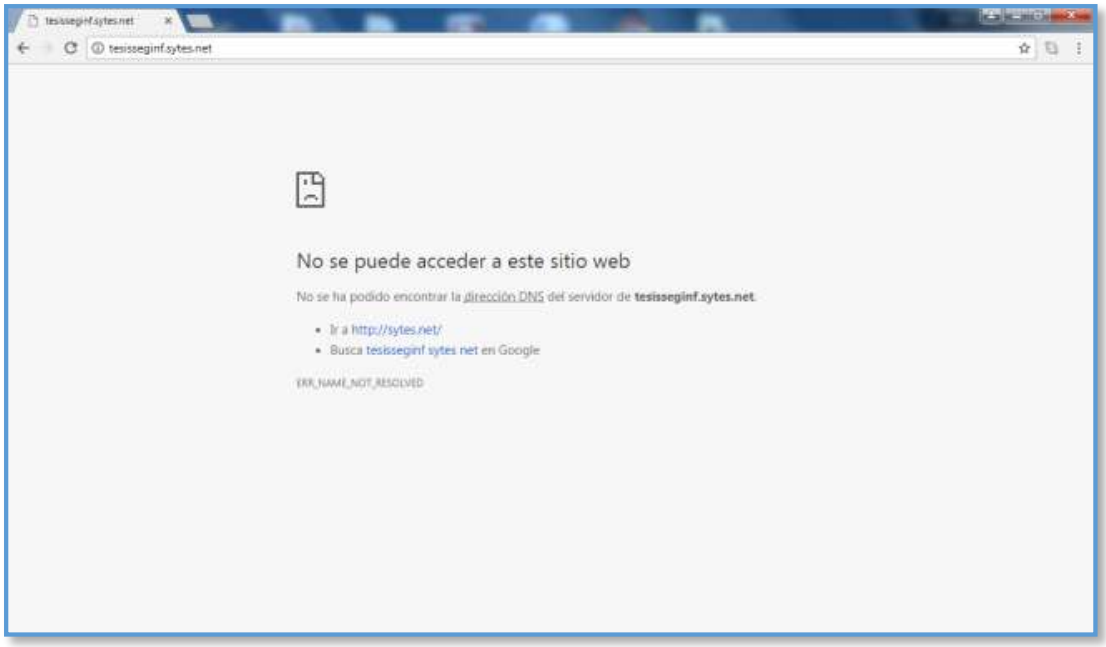


Fuente: Elaboración propia.

El resultado fue el mismo, el día 10 de septiembre entre las 11:36 am y las 12:06 pm, ninguna solicitud pudo ser atendida durante ese lapso de tiempo, con lo cual podemos concluir que los módulos de seguridad apache modsecurity y apache mod evasive no son efectivos al proteger un servidor web de un ataque DDoS.

Los usuarios no pudieron acceder a la página web durante los 30 minutos del ataque.

Figura 49: *Sin acceso a la página web durante el ataque DDoS con módulo Evasive implementado.*



Fuente: Elaboración propia.

5.2. MÓDULO DE SEGURIDAD MOD_QOS

El resultado fue completamente opuesto con el módulo de seguridad apache mod_qos, este módulo mostro mayor efectividad al momento de proteger el servidor web apache de los ataques DDoS mediante el script Slowloris. A partir de ese momento se procedió a realizar el diseño pre test - post test, con esto podíamos demostrar la diferencia que existía entre un servidor web apache sin ninguna protección y la de un servidor web que poseía la protección del módulo de seguridad apache mod_qos.

5.2.1. DISEÑO PRE TEST

Una vez definido el módulo de seguridad a emplear, utilizamos el diseño pre test (sin protección alguna) y se realizaron varios ataques al servidor web.

5.2.1.1. ATAQUE DE 5 MINUTOS

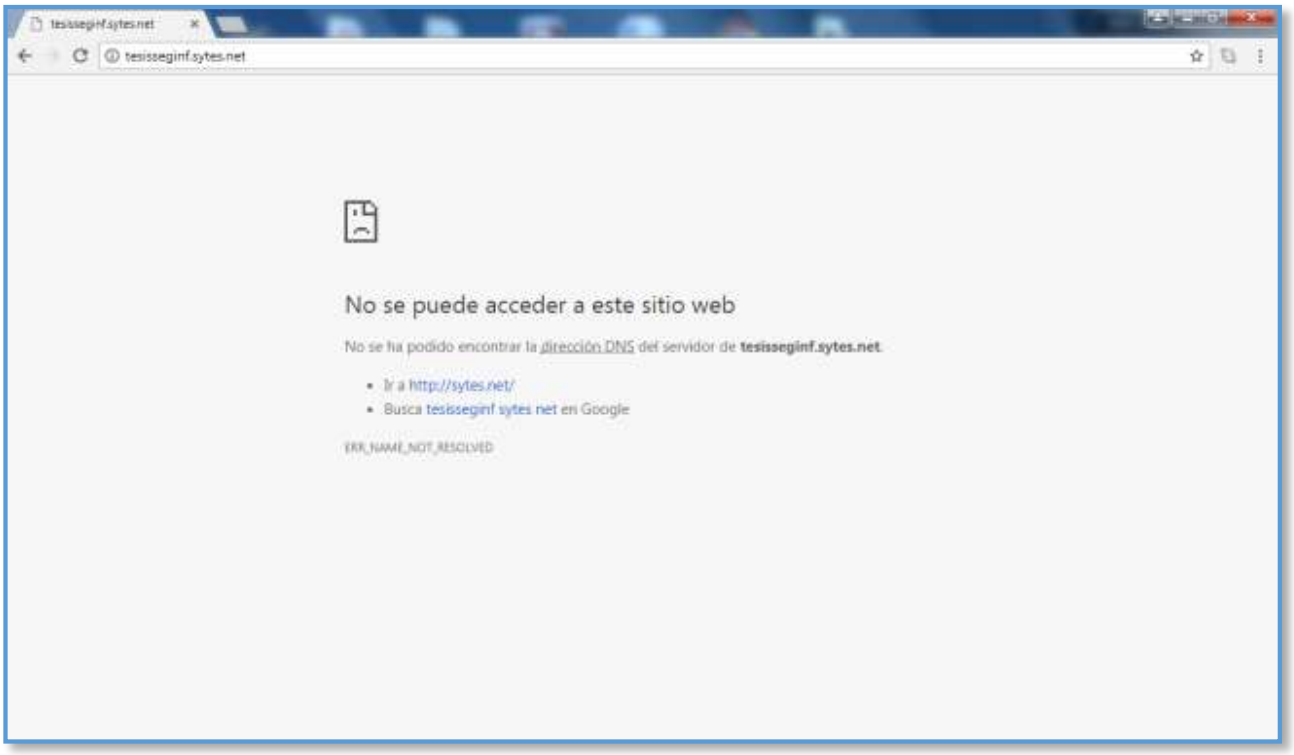
En primer lugar, se realizó el ataque de 5 minutos, este ataque se realizó sin protección y se obtuvo lo siguiente

Figura 50: *Ataque pre-test de 5 minutos.*

Fuente: Elaboración propia.

Se puede observar que durante 5 minutos el servidor web no responderá a ninguna solitud. Durante las 10:18 y las 10:23 horas ningún usuario puede acceder a la página.

Figura 51: *Sin acceso a la página web durante el ataque de 5 minutos sin protección.*



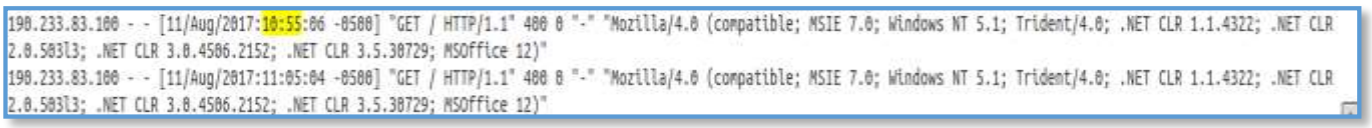
Fuente: Elaboración propia.

5.2.1.2. ATAQUE DE 10 MINUTOS

A si mismo se repitió esta secuencia de ataques con un tiempo de 10 minutos, los resultados fueron similares.

Al ingresar al log Access del servidor web obtenemos lo siguiente:

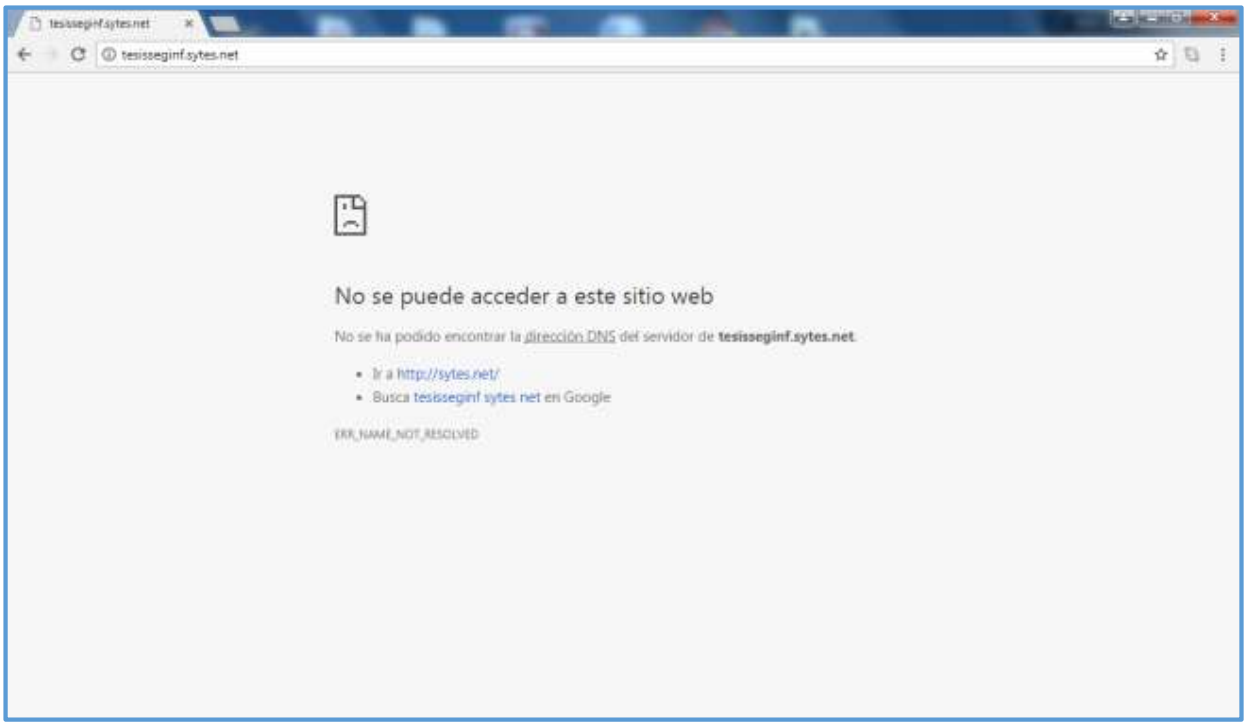
Figura 52: *Ataque pre-test de 10 minutos.*



Fuente: Elaboración propia.

Se concluye que durante 10 minutos de ataque DDoS desde las 10:55 a las 11:05 horas del día 11 de agosto del 2017, la página web no responde correctamente, con lo cual ningún usuario puede acceder a la página web.

Figura 53: *Sin acceso a la página web durante el ataque de 10 minutos sin protección.*

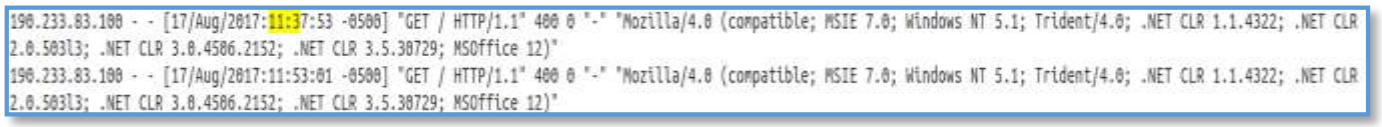


Fuente: Elaboración propia.

5.2.1.3. ATAQUE DE 15 MINUTOS

A si mismo se repitió esta secuencia de ataques con un tiempo de 15 minutos, al ingresar al log Access del servidor web durante el periodo de ataque se observa lo siguiente:

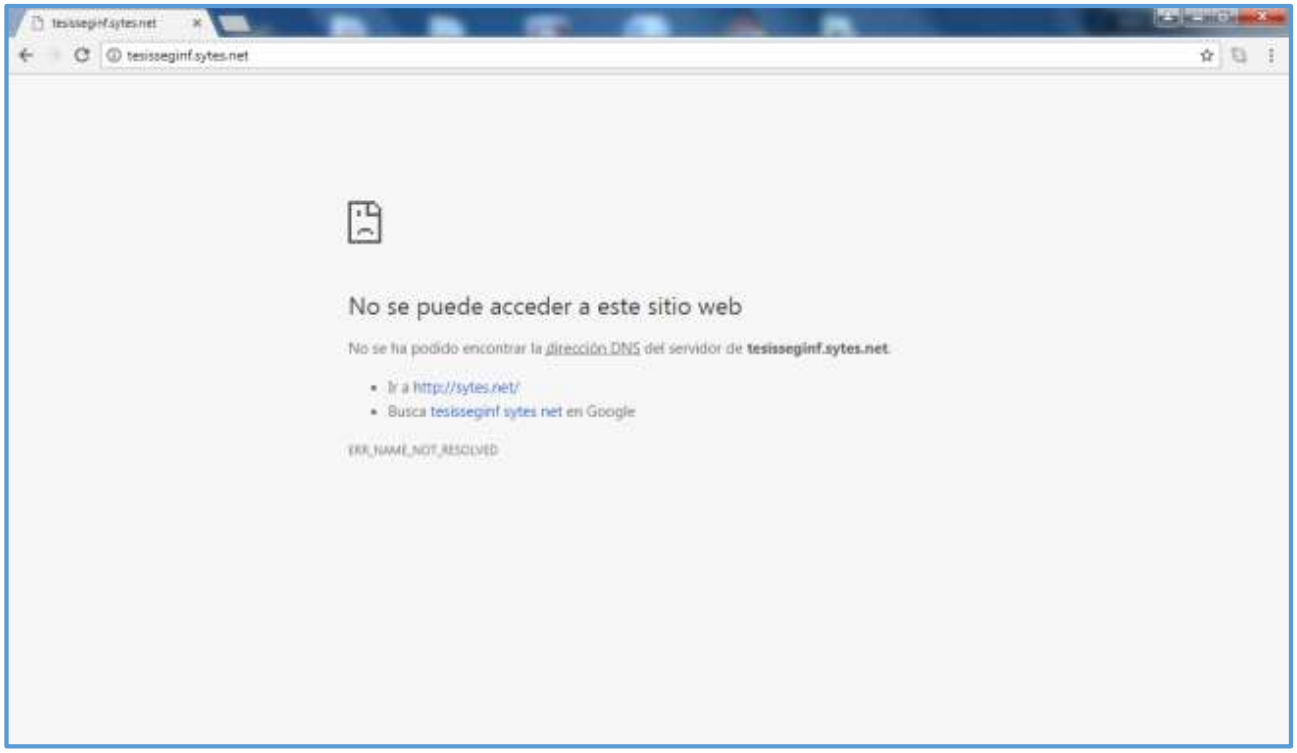
Figura 54: *Ataque pre-test de 15 minutos.*



Fuente: Elaboración propia.

Dentro de las 11:38 y 11:53 horas de ataque del día 17 de agosto del 2017, el servidor web no responde a ninguna solicitud de usuarios, por lo tanto, resulta inaccesible por ese periodo de tiempo.

Figura 55: *Sin acceso a la página web durante el ataque de 15 minutos sin protección.*

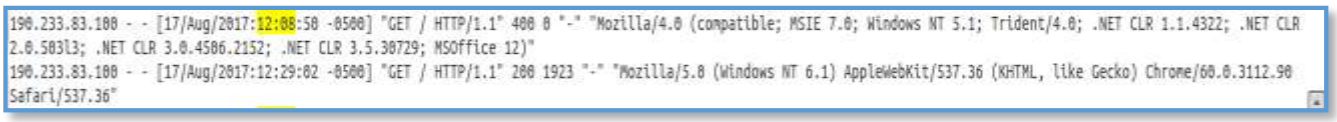


Fuente: Elaboración propia.

5.2.1.4. ATAQUE DE 20 MINUTOS

Se realizó la secuencia de ataques para un tiempo de 20 minutos, al ingresar al log Access del servidor web durante el periodo de ataque se observa lo siguiente:

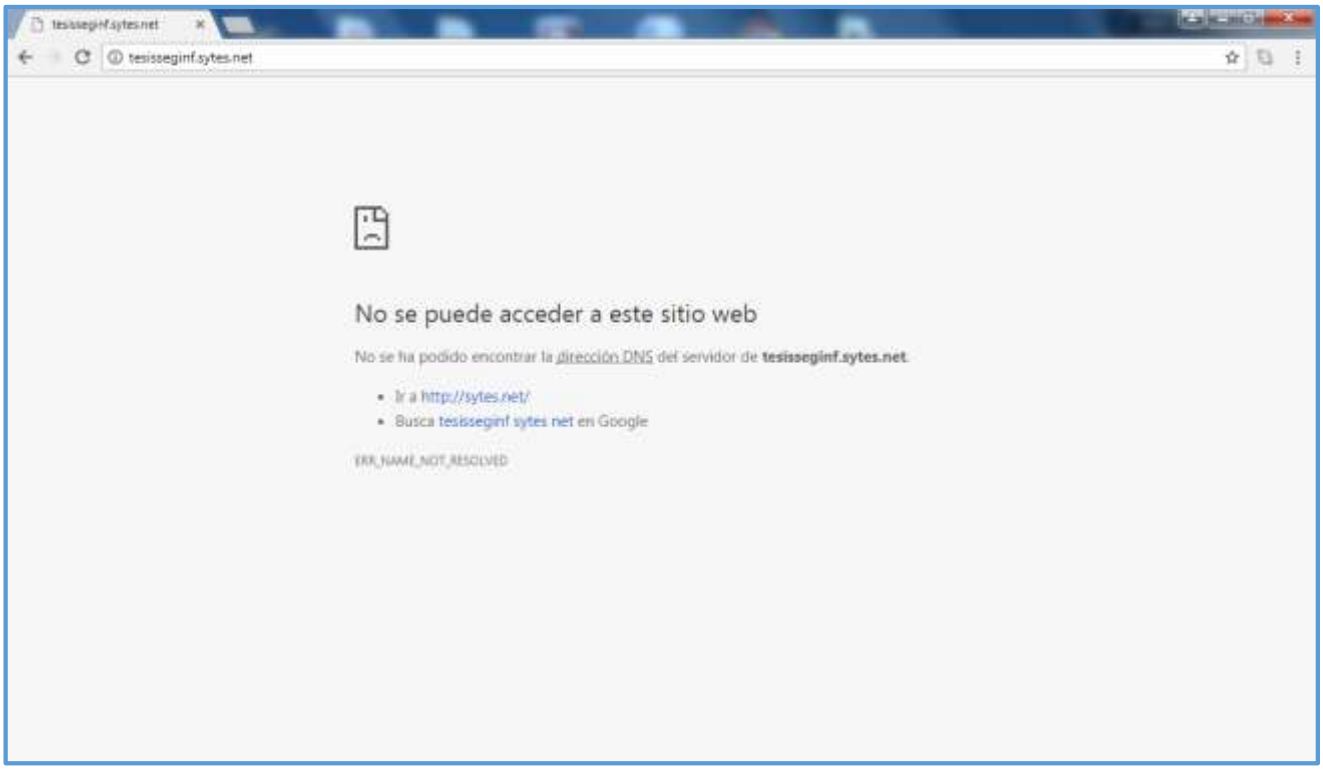
Figura 56*: Ataque pre-test de 20 minutos.*



Fuente: Elaboración propia.

Dentro de las 12:09 y 12:29 horas de ataque del día 17 de agosto del 2017, el servidor web no responde a ninguna solicitud de usuarios, por lo tanto, resulta inaccesible por ese periodo de tiempo.

Figura 57: *Sin acceso a la página web durante el ataque de 20 minutos sin protección.*

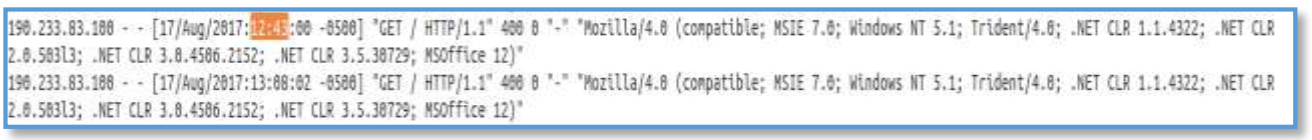


Fuente: Elaboración propia.

5.2.1.5. ATAQUE DE 25 MINUTOS

Se realizó la secuencia de ataques para un tiempo de 25 minutos, al ingresar al log Access del servidor web durante el periodo de ataque se observa lo siguiente:

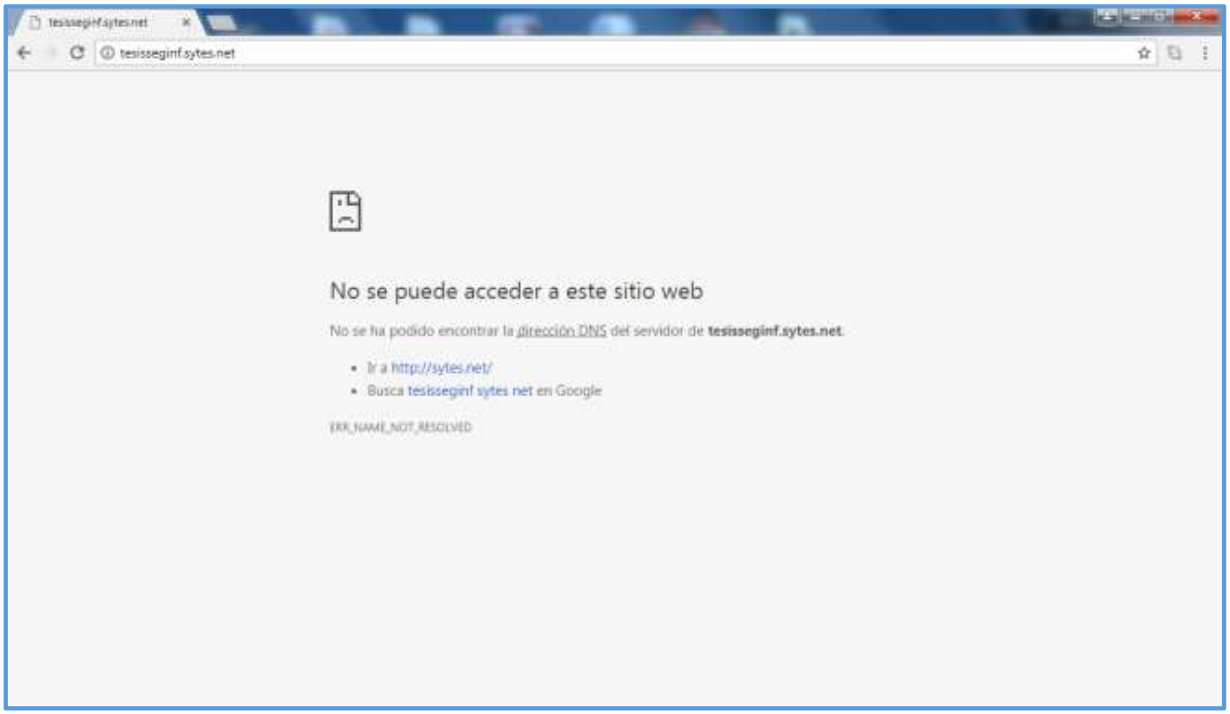
Figura 58*: Ataque pre-test de 25 minutos.*



Fuente: Elaboración propia.

Dentro de las 12:43 y 13:08 horas de ataque del día 17 de agosto del 2017, el servidor web no responde a ninguna solicitud de usuarios, por lo tanto, resulta inaccesible por ese periodo de tiempo.

Figura 59: *Sin acceso a la página web durante el ataque de 25 minutos sin protección.*



Fuente: Elaboración propia.

5.2.1.6. ATAQUE DE 30 MINUTOS

Se realizó la secuencia de ataques para un tiempo de 30 minutos, al ingresar al log Access del servidor web durante el periodo de ataque se observa lo siguiente:

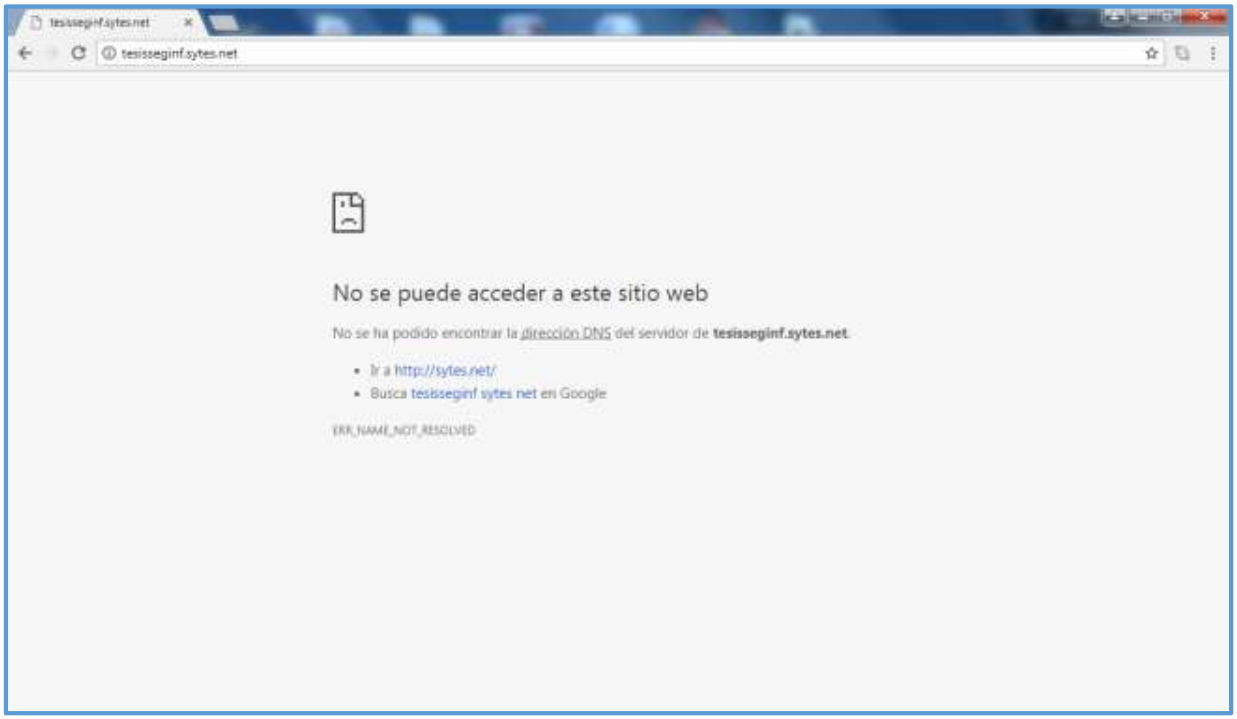
Figura 60: *Ataque pre-test de 30 minutos.*

```
190.233.83.100 - - [19/Aug/2017:11:23:59 -0500] "GET / HTTP/1.1" 400 0 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR
2.0.503l3; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)"
190.233.83.100 - - [19/Aug/2017:11:54:58 -0500] "GET / HTTP/1.1" 400 0 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR
2.0.503l3; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)"
```

Fuente: Elaboración propia.

Dentro de las 11.24 y 11:54 horas de ataque del día 19 de agosto del 2017, el servidor web no responde a ninguna solicitud de usuarios, por lo tanto, resulta inaccesible por ese periodo de tiempo.

Figura 61: *Sin acceso a la página web durante el ataque de 30 minutos sin protección.*



Fuente: Elaboración propia.

5.2.1.7. ATAQUE DE 60 MINUTOS

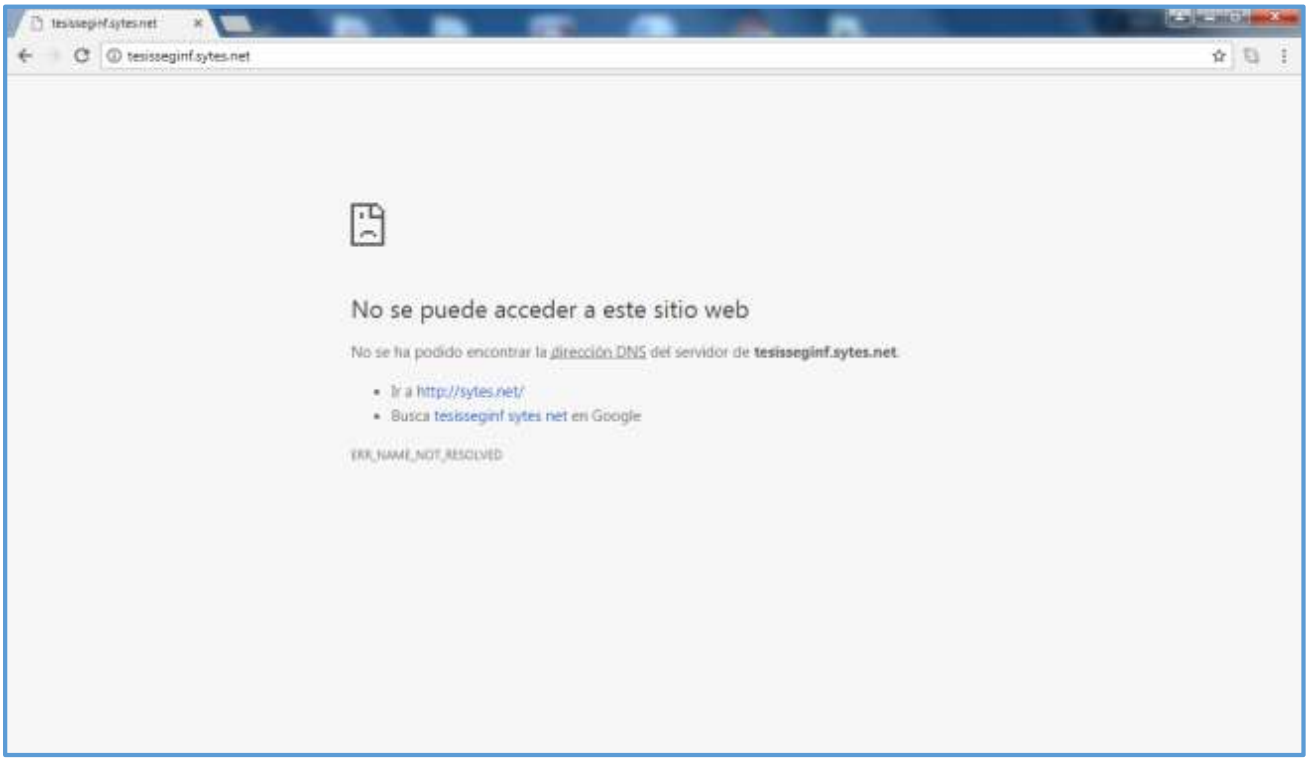
Al acceder al log Access del servidor web, se muestra lo siguiente durante los ataques de 60 minutos.

Figura 62: *Ataque pre-test de 60 minutos.*

Fuente: Elaboración propia.

Se concluye que durante 60 minutos de ataque DDoS desde las 12:16 a las 13:16 horas del día 19 de agosto del 2017, la página web no responde correctamente ante las solicitudes de los usuarios.

***Figura 63**: Sin acceso a la página web durante el ataque de 60 minutos sin protección.*



Fuente: Elaboración propia.

5.2.1.8. ATAQUE DE 90 MINUTOS

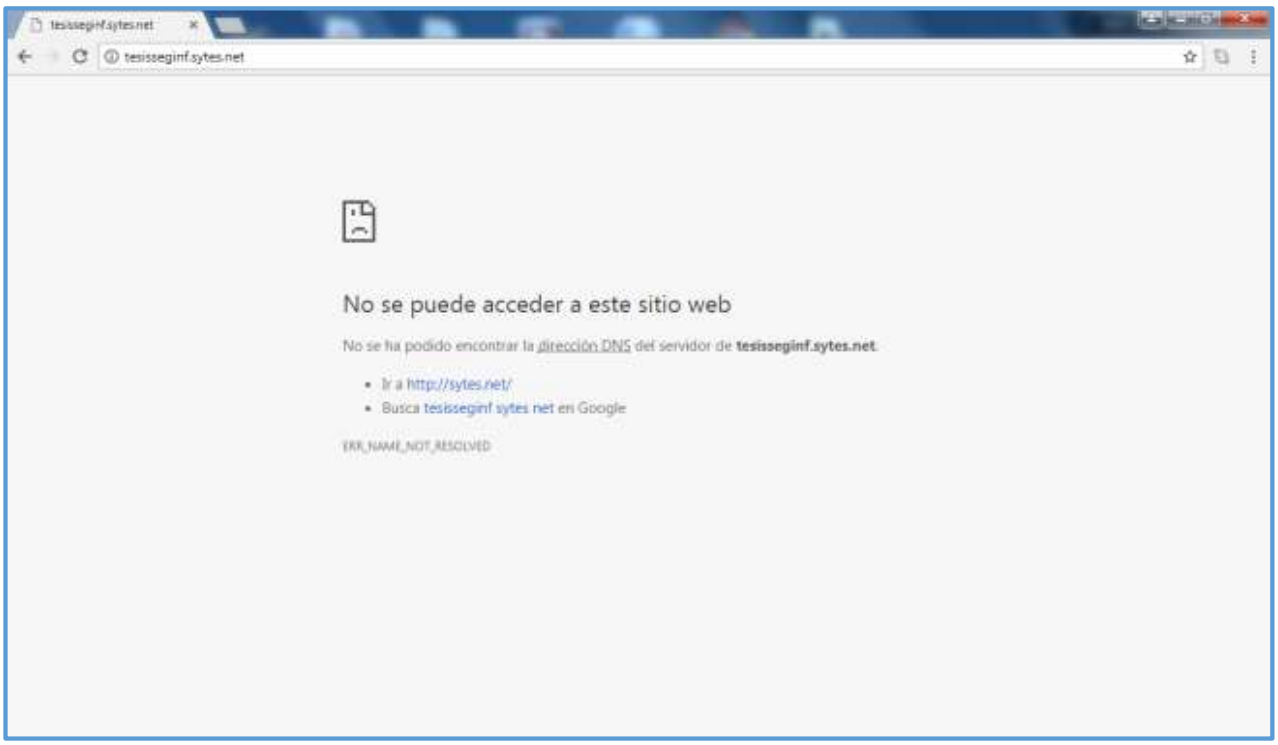
Para concluir con la fase de pre test, se realizaron los ataques de 90 minutos y obtuvimos los siguientes resultados:

***Figura 64:** Ataque pre-test de 90 minutos.*

Fuente: Elaboración propia.

Se concluye que durante 90 minutos de ataque DDoS desde las 15:55 a las 17:25 horas del día 21 de agosto del 2017, la página web no responde correctamente.

Figura 65: *Sin acceso a la página web durante el ataque de 90 minutos sin protección.*



Fuente: Elaboración propia.

Para finalizar podemos ver que, durante la realización de los ataques, no existen accesos positivos a la página web.

Tiempos	Número de accesos positivos
5 minutos	0
10 minutos	0
15 minutos	0
20 minutos	0
25 minutos	0
30 minutos	0
60 minutos	0
90 minutos	0

Tabla 5: *Número de accesos positivos por cada tiempo en el pre-test.*

De esta manera se concluye que el servidor web apache no responde a las solicitudes enviadas por los usuarios en un diseño pre test, esto puede perjudicar enormemente a una entidad sino toma en cuenta las medidas de seguridad óptimas.

5.2.2. DISEÑO POST TEST

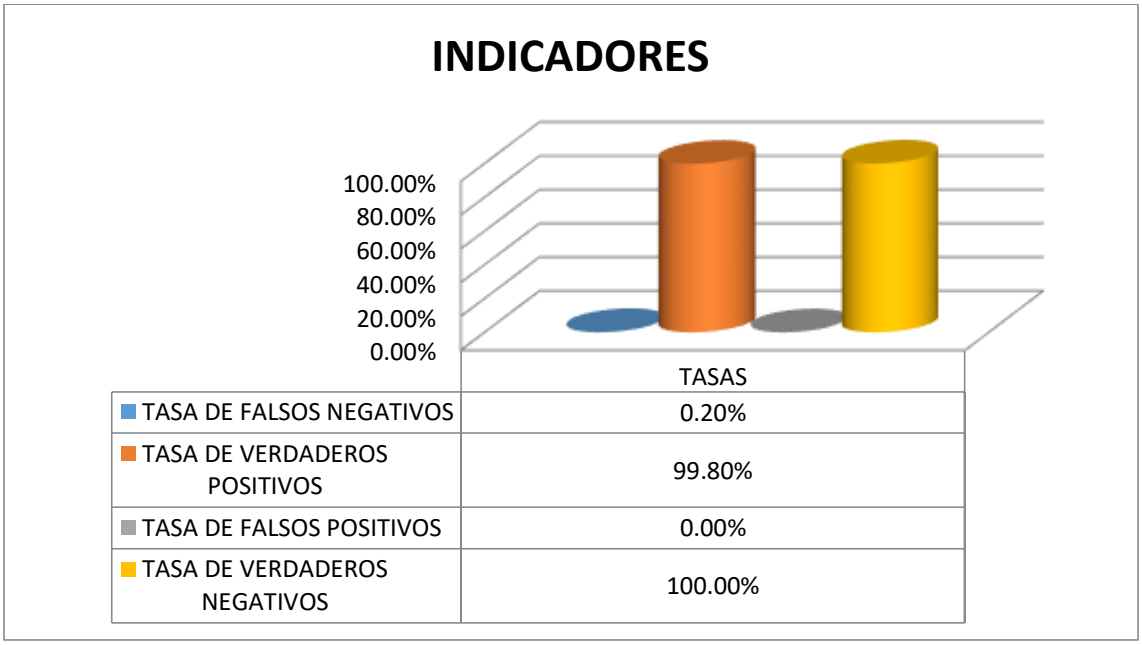
Una vez demostrado que el servidor web por sí solo no puede responder a las solicitudes de los usuarios durante un ataque DDoS a través del script Slowloris, se adaptó el diseño post test, el cual implementó el módulo de seguridad apache mod_qos. A partir de ese momento se buscó medir el nivel de efectividad que poseía este módulo para diversos tiempos, se llevaron a cabo 400 ataques de acuerdo a la muestra establecida previamente, considerando 8 tiempos de 5, 10, 15, 20, 25, 30, 60 y 90 minutos respectivamente.

Para cada tiempo se consideraron 4 indicadores que nos permitieron determinar el nivel de efectividad del módulo apache mod_qos ante los diversos tiempos especificados, los indicadores considerados fueron Tasa de Verdaderos Positivos (VP), Tasa de Verdaderos Negativos, Tasa de Falsos Positivos, Tasa de Falsos Negativos (FN).

5.2.2.1. ATAQUE DE 5 MINUTOS

A continuación, mostraremos los resultados obtenidos para el primer ataque que fue de 5 min y se obtuvieron los siguientes resultados:

Figura 66: *Ataque post-test de 5 minutos.*



	TASAS
TASA DE FALSOS NEGATIVOS	0.20%
TASA DE VERDADEROS POSITIVOS	99.80%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

Fuente: Elaboración propia.

Estos indicadores muestran el desempeño del módulo apache mod_qos y tendrán la siguiente interpretación:

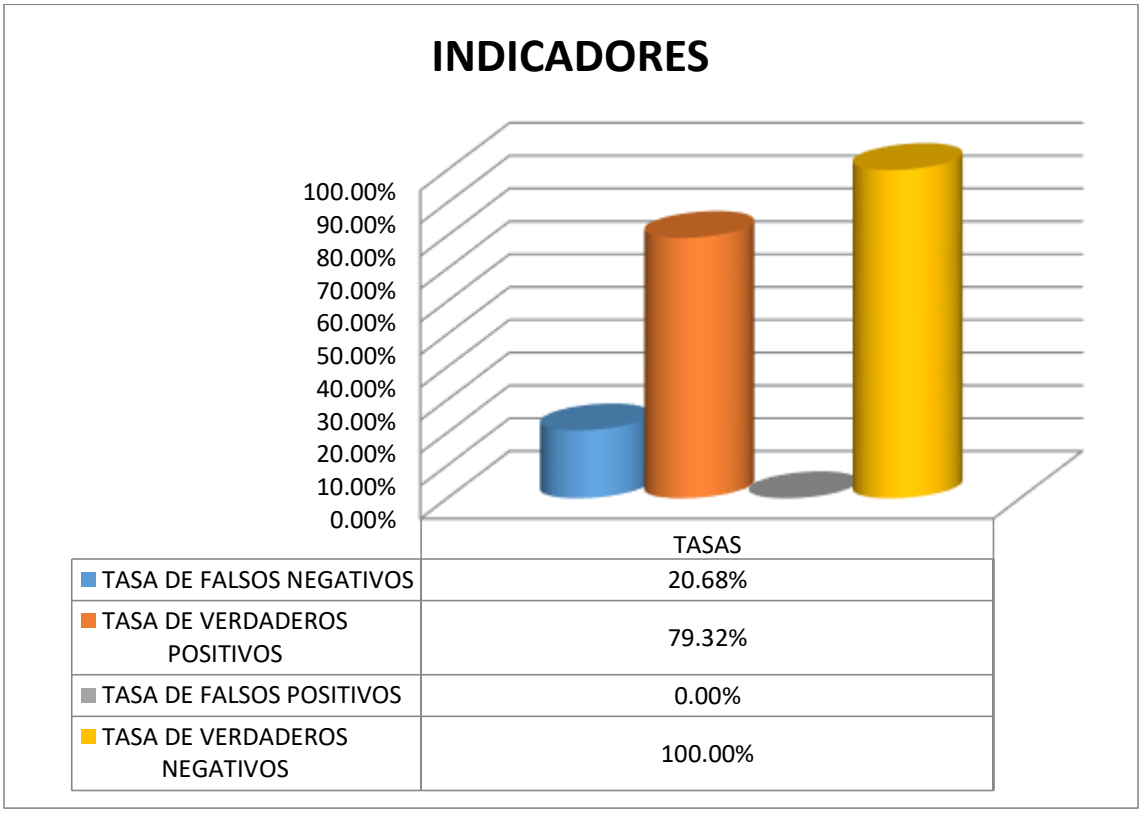
Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 0,20%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 99,80%.

Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.2. ATAQUE DE 10 MINUTOS

El resultado para el ataque de 10 minutos fue el siguiente:

Figura 67: *Ataque post-test de 10 minutos.*



TASA DE FALSOS NEGATIVOS	20.68%
TASA DE VERDADEROS POSITIVOS	79.32%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

Fuente: Elaboración propia.

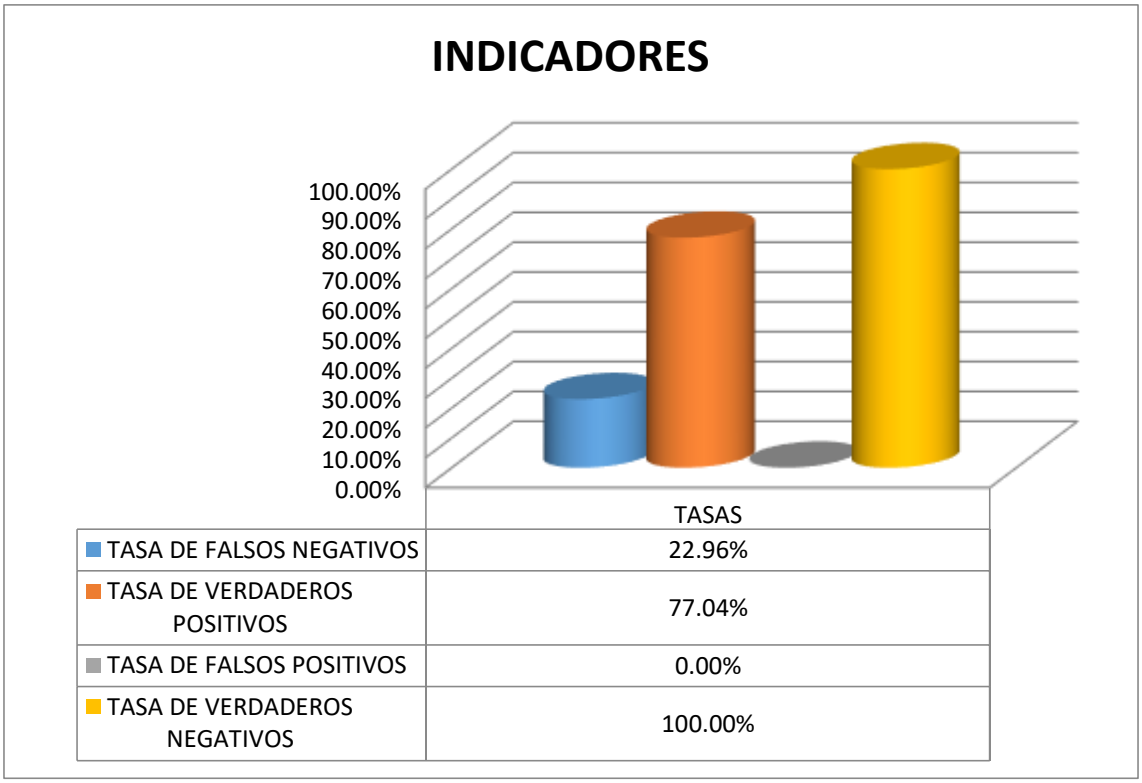
Podemos interpretarlo de la siguiente manera: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 20,68%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 79,32%.

Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.3. ATAQUE DE 15 MINUTOS

Durante el ataque de 15 minutos se obtuvieron los siguientes resultados:

Figura 68: *Ataque post-test de 15 minutos.*



	TASAS
TASA DE FALSOS NEGATIVOS	22.96%
TASA DE VERDADEROS POSITIVOS	77.04%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

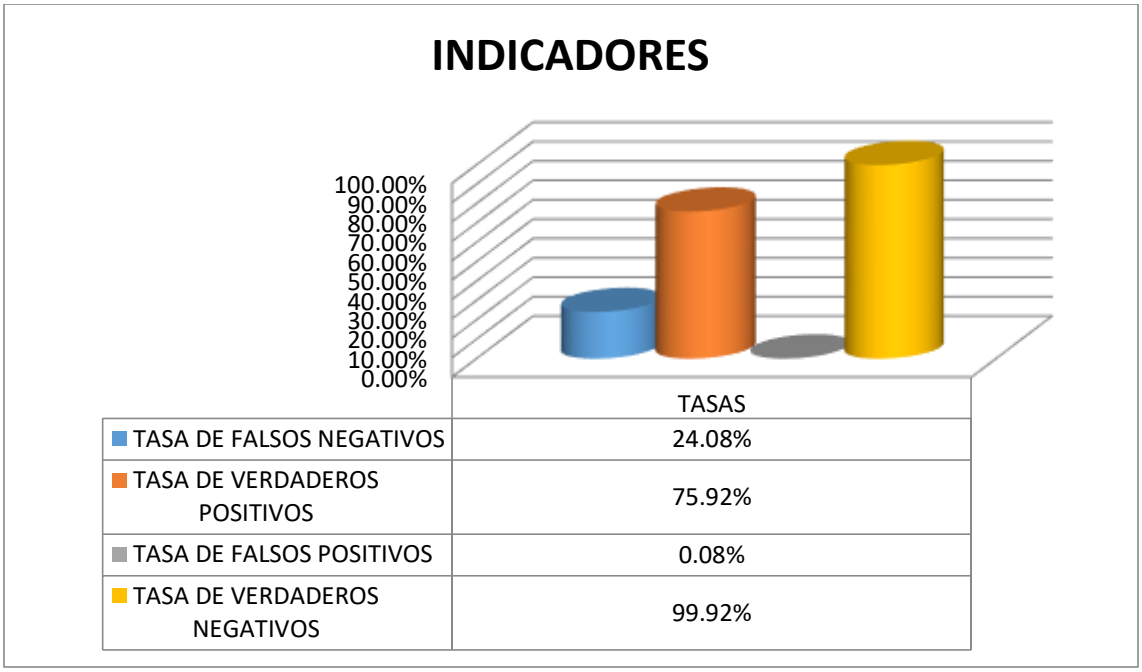
Fuente: Elaboración propia.

Podemos interpretarlo de la siguiente manera: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 22,96%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 77,04%.
Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.4. ATAQUE DE 20 MINUTOS

Durante el ataque de 20 minutos se obtuvieron los siguientes resultados:

Figura 69: *Ataque post-test de 20 minutos.*



TASA DE FALSOS NEGATIVOS	24.08%
TASA DE VERDADEROS POSITIVOS	75.92%
TASA DE FALSOS POSITIVOS	0.08%
TASA DE VERDADEROS NEGATIVOS	99.92%

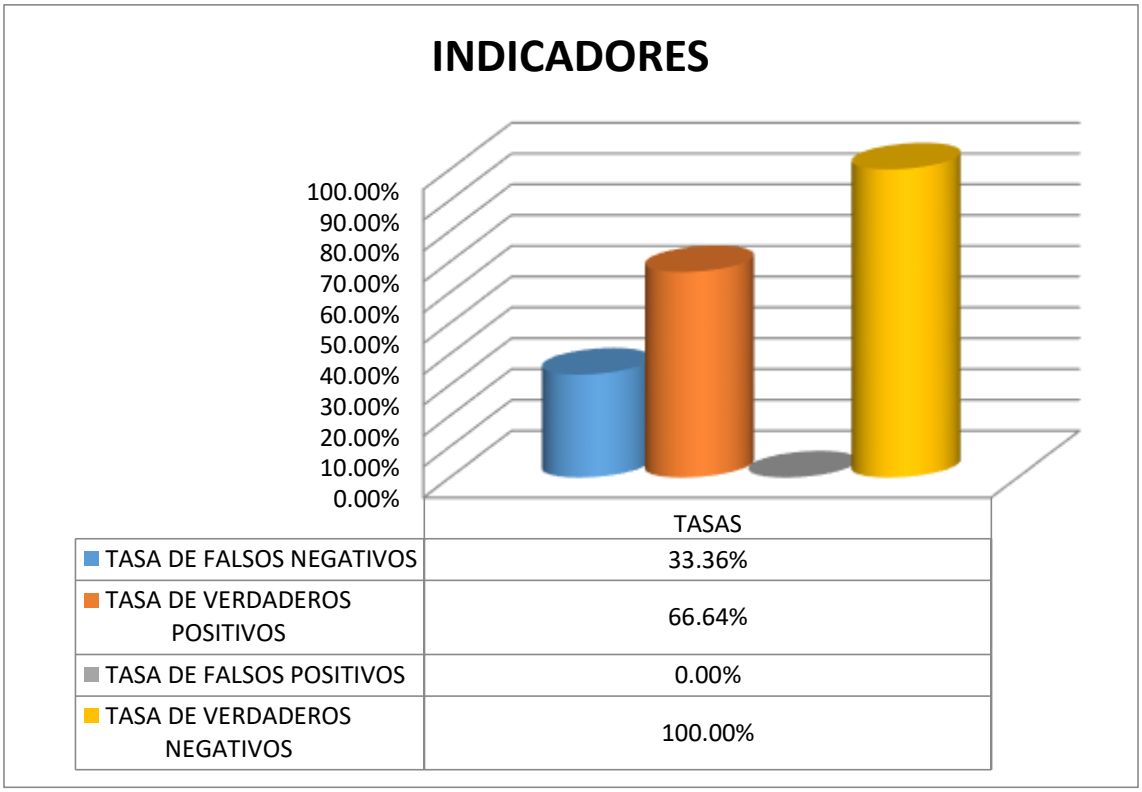
Fuente: Elaboración propia.

La interpretación seria la siguiente: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 24,08%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 75,92%.
Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0,08% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 99,92%.

5.2.2.5. ATAQUE DE 25 MINUTOS

Durante el ataque de 25 minutos se obtuvieron los siguientes resultados:

Figura 70: *Ataque post-test de 25 minutos.*



	TASAS
TASA DE FALSOS NEGATIVOS	33.36%
TASA DE VERDADEROS POSITIVOS	66.64%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

Fuente: Elaboración propia.

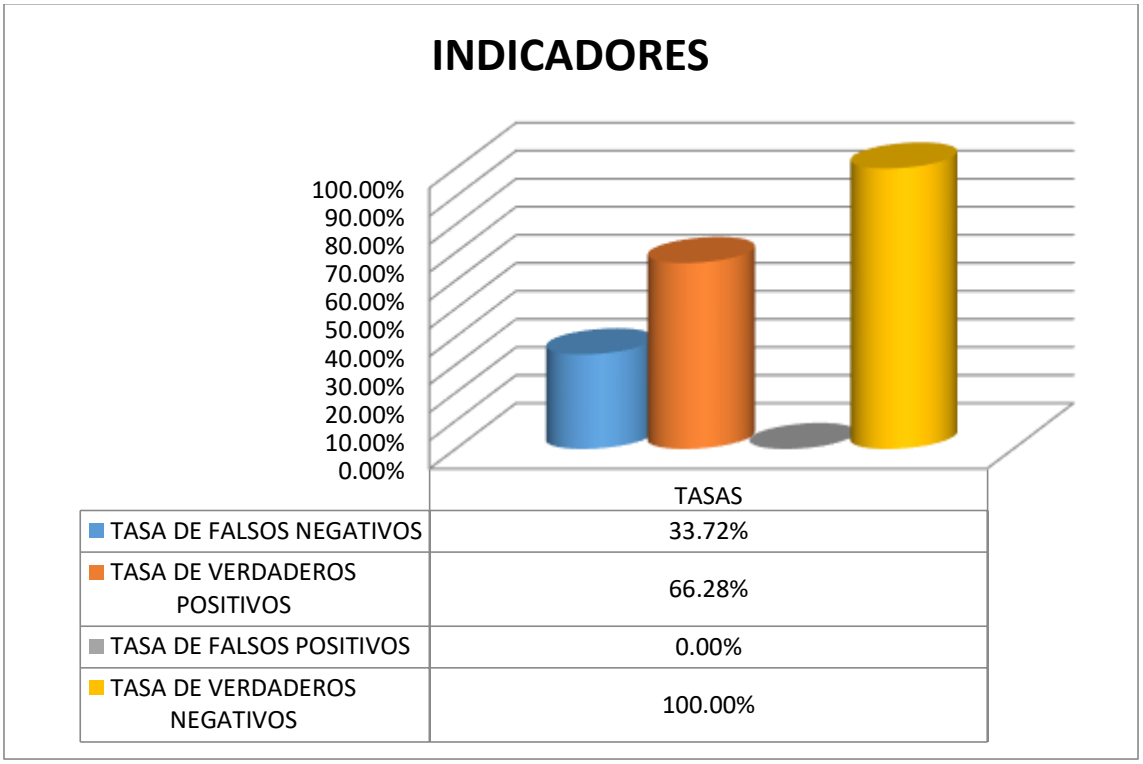
El siguiente grafico tendría la siguiente interpretación: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 33,36%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 66,64%.

Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.6. ATAQUE DE 30 MINUTOS

Posteriormente al realizarse el ataque de 30 minutos se obtuvieron los siguientes resultados:

Figura 71: *Ataque post-test de 30 minutos.*



Fuente: Elaboración propia.

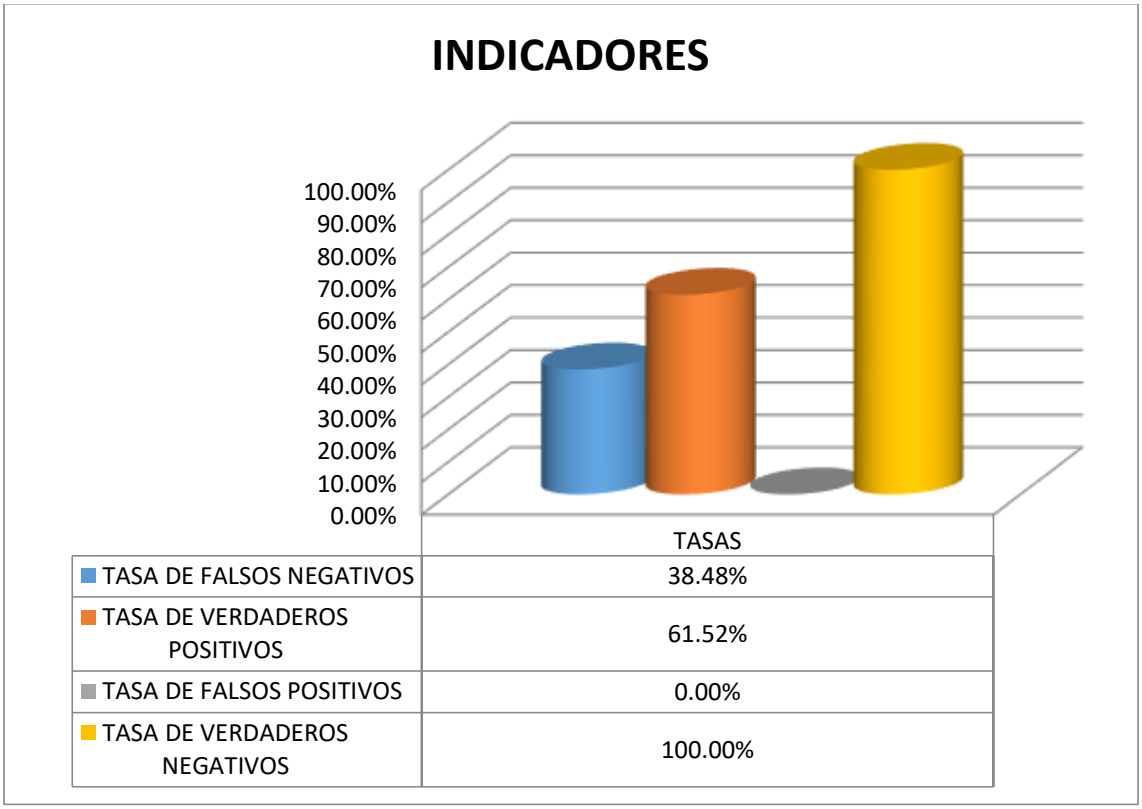
El siguiente grafico tendría la siguiente interpretación: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 33,72%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 66,28%.

Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.7. ATAQUE DE 60 MINUTOS

Luego se realizó el ataque de 60 minutos obteniéndose los siguientes resultados:

Figura 72: *Ataque post-test de 60 minutos.*



	TASAS
TASA DE FALSOS NEGATIVOS	38.48%
TASA DE VERDADEROS POSITIVOS	61.52%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

Fuente: Elaboración propia.

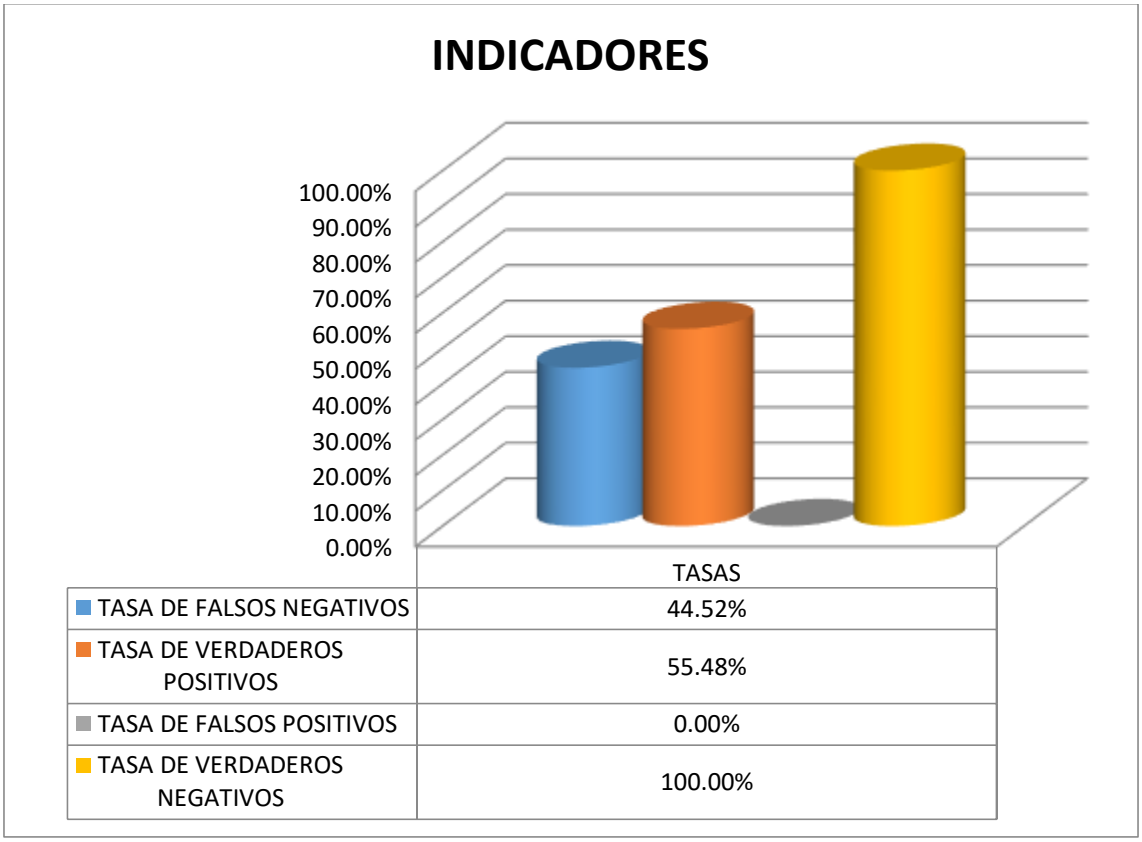
La interpretación será la siguiente: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 38,48%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 61,52%.

Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

5.2.2.8. ATAQUE DE 90 MINUTOS

Finalmente se realizó el ataque de 90 minutos obteniéndose los siguientes resultados:

Figura 73: *Ataque post-test de 90 minutos.*



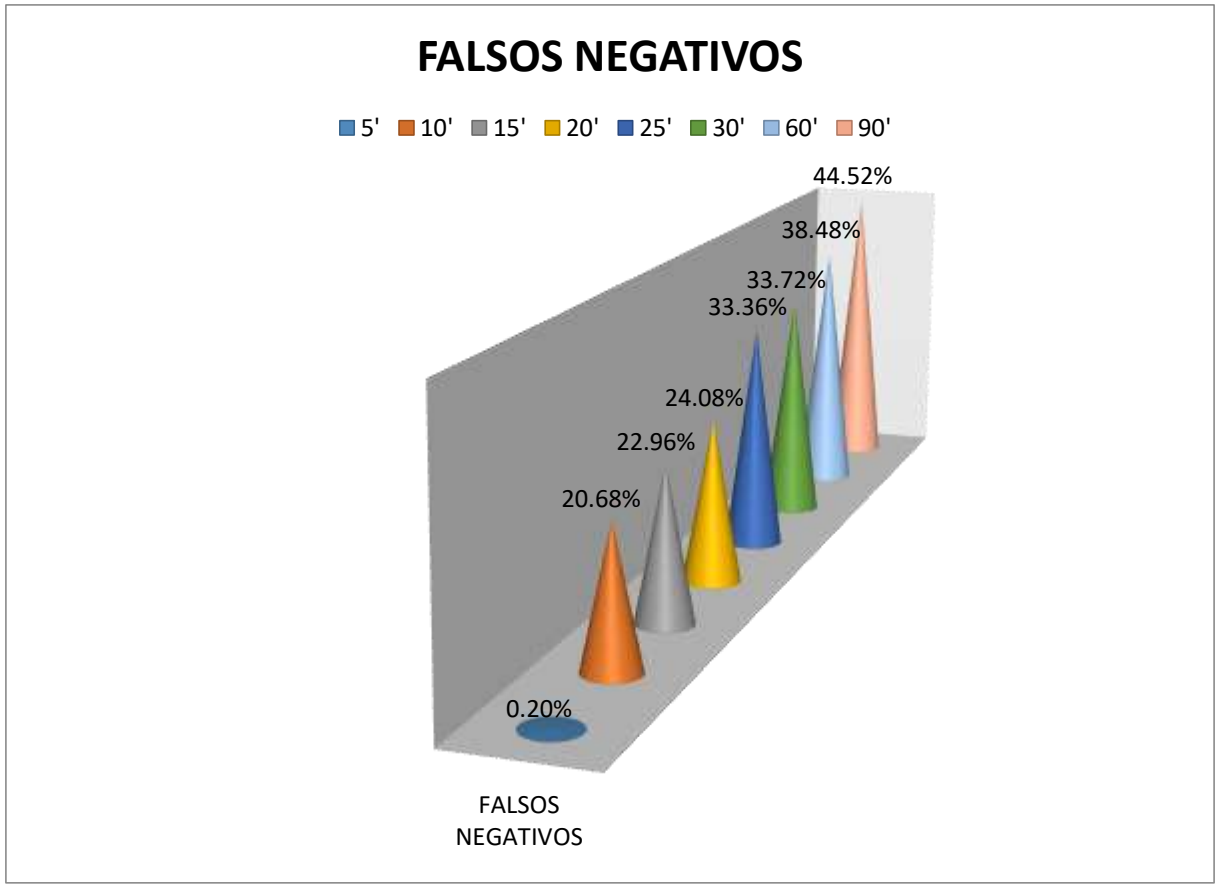
	TASAS
TASA DE FALSOS NEGATIVOS	44.52%
TASA DE VERDADEROS POSITIVOS	55.48%
TASA DE FALSOS POSITIVOS	0.00%
TASA DE VERDADEROS NEGATIVOS	100.00%

Fuente: Elaboración propia.

Podemos interpretarlo de la siguiente manera: Durante la realización de los ataques DDoS se determinó que el porcentaje de ataques que no fueron detectados fue del 44,52%, a su vez se concluye que el porcentaje de ataques correctamente detectados fue del 55,48%. Además, se concluye que el porcentaje de tráfico legítimo detectado incorrectamente como ataque es del 0% y el porcentaje de tráfico normal correctamente identificado como tráfico normal es del 100%.

Una vez analizados todos los índices expuestos presentaremos la evolución de los porcentajes de acuerdo a los tiempos de ataque, como se evidencia a continuación:

Figura 74: *Falsos Negativos – Ataques que no fueron detectados.*

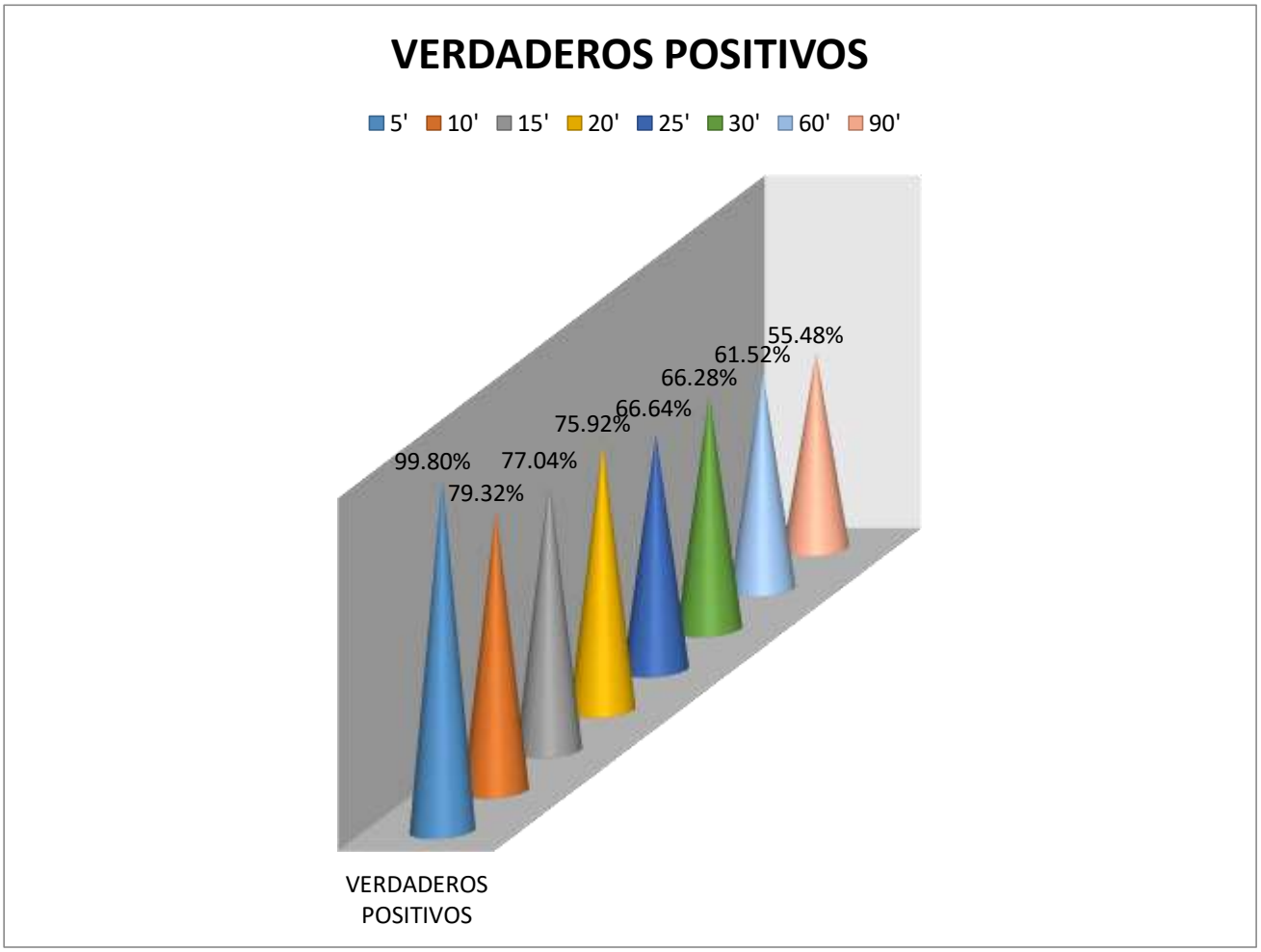


Fuente: Elaboración propia.

De acuerdo al grafico podemos identificar un relativo crecimiento en la tasa de los falsos negativos, podemos concluir de dicho grafico que la tasa de falsos negativos a lo largo de los 8 tiempos se interpretaría de la siguiente manera: El porcentaje de ataques que no fueron detectados es directamente proporcional a la duración de los ataques.

A continuación, analizaremos la tasa de los verdaderos positivos, para los 8 tiempos de ataques realizados.

Figura 75: *Verdaderos Positivos – Ataques correctamente detectados.*



Fuente: Elaboración propia.

De acuerdo al grafico podemos identificar un relativo decrecimiento en la tasa de los verdaderos positivos, podemos concluir de dicho grafico que la tasa de verdaderos positivos a lo largo de los 8 tiempos se interpretaría de la siguiente manera:

El porcentaje de ataques correctamente detectados es inversamente proporcional a la duración de los ataques.

CAPÍTULO VI

VI. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

A partir de los distintos experimentos realizados con el conjunto de datos, se ha llegado a las siguientes conclusiones:

- En primer lugar podemos concluir que se logro Identificar correctamente los ataques de denegación de servicio distribuido en el servidor web Apache, mediante el log de error, una vez instalado el módulo de seguridad mod_qos.

- Una vez Implementado el servidor web Apache se logró verificar la existencia de las vulnerabilidades de DDoS, dichas vulnerabilidades se evidencian en la prueba pre test de nuestro diseño. Al evidenciarse las vulnerabilidades estas podrían significar un indicador altamente peligroso para cualquier entidad que no tome las medidas correspondientes.

- Podemos concluir que luego de analizar los módulos de seguridad Apache, la herramienta de seguridad que mejores resultados mostro es el módulo de seguridad mod_qos, este módulo de seguridad brinda mayor protección contra los ataques DDoS.

- Se concluye que mediante la implementación del módulo de seguridad apache mod_qos el servidor web responde satisfactoriamente a las solicitudes enviadas por los usuarios, inclusive durante la realización de ataques DDoS en tiempo real a través del script Slowloris.

- Como conclusión final podemos decir que se logro Implementar satisfactoriamente el módulo de seguridad apache mod_qos para prevenir y detectar ataques de tipo DDoS dirigidos al servidor web http://tesisseginf.sytes.net.

6.2. RECOMENDACIONES

- Teniendo en cuenta los buenos resultados obtenidos con la investigación, se sugiere a futuras empresas llevar a cabo la planificación y aplicación de esta herramienta de seguridad que garantiza la continuidad y desempeño del negocio.

- Se recomienda a futuros estudiantes que muestren interés en la tesis que continúen con este tipo de investigaciones y a su vez busquen mejores soluciones ante la problemática planteada, de esa forma poder hacer comparaciones entre los resultados arrojados.

VII. REFERENCIAS BIBLIOGRÁFICAS

- Tello Padilla, R. A. (2013). Esquema de seguridad contra ataques DoS y DDoS, Caso: Diario de Quintana Roo (Tesis de grado). Universidad de Quintana Roo, División de Ciencias e Ingeniería. Chetumal, México.

- Campo Giralte, L. (2009). Una arquitectura distribuida para la detección, comunicación y mitigación de la denegación de servicio. (Tesis doctoral). Escuela Técnica Superior de Ingeniería Informática. Universidad Rey Juan Carlos.

- Britos José, D. (2010). Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico (Tesis de maestría).

- Estrella Quijije, G. D., (2011). Diseño del Prototipo de una Honeypot Virtual que permitirá mejorar el esquema de seguridad en las redes de la carrera de Ingeniería en sistemas computacionales y Networking de la Universidad de Guayaquil (Tesis de grado). Facultad de Ciencias Matemáticas y Físicas de la carrera de Ingeniería en Sistemas Computacionales Y Networking. Guayaquil – Ecuador.

- Gago Padreny, I. (2015). Sistema de Detección de Ataques DDoS en Tor (Trabajo de fin de Grado). Universidad Complutense de Madrid. Madrid.

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

- QoS. *Mod_qos.* Consultado en: http://mod-qos.sourceforge.net/

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

- Boulevard, Wilson. *Protocolo de Control de Transmisión.* Consultado en: https://tools.ietf.org/html/rfc793.

- Microsoft TechNet. *Sistema de nombres de dominio.* Consultado en: https://technet.microsoft.com/es-es/network/bb629410.aspx

- The Apache HTTP Server Project. *Apache httpd Modules.* Consultado en http://httpd.apache.org/modules/

- The Apache HTTP Server Project. *About the Apache HTTP Server Project* .Consultado en: http://httpd.apache.org/ABOUT_APACHE.html

- Echeverri, G. A., O., L. F., Trujillo, M. L., & Marulanda, C. E. (2010). Modelo híbrido de neuroclasificación y clustering en el problema de detección de intrusiones. Vector, Pág 69,77.

- A. Ghorbani, W. Lu y M. Tavallaee, Evaluation Criteria. Network Intrusion Detection and Prevention. Concepts and Techniques. Advances in Information Security, Springer US, pp. 161-183, 2010.

- 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.

- Hoyos Llanos, M. (2015). Prototipo de detección de ataques distribuidos de denegación de servicios (DDOS) a partir de máquinas de aprendizaje (Tesis de Maestría). Universidad Autónoma de Manizales, Colombia.

ANEXOS

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (5 MINUTOS)**

	Abril	Periodo de Tiempo (5')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	20-abr-2017	9:57:00 AM	10:02:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
2	20-abr-2017	10:15:00 AM	10:20:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
3	20-abr-2017	10:25:00 AM	10:30:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
4	20-abr-2017	10:34:00 AM	10:39:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
5	20-abr-2017	10:44:00 AM	10:49:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
6	20-abr-2017	11:00:00 AM	11:05:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
7	20-abr-2017	11:17:00 AM	11:22:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
8	20-abr-2017	11:40:00 AM	11:45:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
9	20-abr-2017	11:49:00 AM	11:54:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
10	20-abr-2017	11:57:00 AM	12:02:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
11	20-abr-2017	12:20:00 PM	12:25:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
12	20-abr-2017	12:35:00 PM	12:40:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
13	20-abr-2017	12:43:00 PM	12:48:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
14	20-abr-2017	12:52:00 PM	12:57:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
15	20-abr-2017	1:01:00 PM	1:06:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
16	20-abr-2017	5:22:00 PM	5:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
17	20-abr-2017	5:30:00 PM	5:35:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
18	20-abr-2017	5:39:00 PM	5:44:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
19	20-abr-2017	6:05:00 PM	6:10:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
20	20-abr-2017	6:12:00 PM	6:17:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
21	20-abr-2017	6:22:00 PM	6:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
22	20-abr-2017	6:32:00 PM	6:37:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
23	20-abr-2017	6:39:00 PM	6:44:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
24	20-abr-2017	6:46:00 PM	6:51:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
25	20-abr-2017	6:53:00 PM	6:58:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
26	20-abr-2017	7:00:00 PM	7:05:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
27	20-abr-2017	7:10:00 PM	7:15:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
28	20-abr-2017	7:22:00 PM	7:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
29	20-abr-2017	7:29:00 PM	7:34:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	5	10,00%	90,00%
30	20-abr-2017	7:38:00 PM	7:43:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
31	22-abr-2017	9:03:00 AM	9:08:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
32	22-abr-2017	9:11:00 AM	9:16:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
33	22-abr-2017	9:19:00 AM	9:24:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
34	22-abr-2017	9:26:00 AM	9:31:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
35	22-abr-2017	9:34:00 AM	9:39:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
36	22-abr-2017	9:42:00 AM	9:47:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
37	22-abr-2017	9:50:00 AM	9:55:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
38	22-abr-2017	9:57:00 AM	10:02:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
39	22-abr-2017	10:04:00 AM	10:09:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
40	22-abr-2017	10:11:00 AM	10:16:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
41	22-abr-2017	10:18:00 AM	10:23:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
42	22-abr-2017	10:25:00 AM	10:30:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
43	22-abr-2017	10:32:00 AM	10:37:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
44	22-abr-2017	10:40:00 AM	10:45:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
45	22-abr-2017	10:47:00 AM	10:52:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
46	22-abr-2017	10:55:00 AM	11:00:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
47	22-abr-2017	11:02:00 AM	11:07:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
48	22-abr-2017	11:09:00 AM	11:14:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
49	22-abr-2017	11:16:00 AM	11:21:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
50	12-jun-2017	7:16:00 PM	7:21:00 PM	0:05:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
									PROMEDIO	0,20%	99,80%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (5 MINUTOS)**

	Abril	Periodo de Tiempo (5')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	20-abr-2017	9:57:00 AM	10:02:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
2	20-abr-2017	10:15:00 AM	10:20:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
3	20-abr-2017	10:25:00 AM	10:30:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
4	20-abr-2017	10:34:00 AM	10:39:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
5	20-abr-2017	10:44:00 AM	10:49:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
6	20-abr-2017	11:00:00 AM	11:05:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
7	20-abr-2017	11:17:00 AM	11:22:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
8	20-abr-2017	11:40:00 AM	11:45:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
9	20-abr-2017	11:49:00 AM	11:54:00 AM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
10	20-abr-2017	11:57:00 AM	12:02:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
11	20-abr-2017	12:20:00 PM	12:25:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
12	20-abr-2017	12:35:00 PM	12:40:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
13	20-abr-2017	12:43:00 PM	12:48:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
14	20-abr-2017	12:52:00 PM	12:57:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
15	20-abr-2017	1:01:00 PM	1:06:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
16	20-abr-2017	5:22:00 PM	5:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
17	20-abr-2017	5:30:00 PM	5:35:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
18	20-abr-2017	5:39:00 PM	5:44:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
19	20-abr-2017	6:05:00 PM	6:10:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
20	20-abr-2017	6:12:00 PM	6:17:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
21	20-abr-2017	6:22:00 PM	6:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
22	20-abr-2017	6:32:00 PM	6:37:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
23	20-abr-2017	6:39:00 PM	6:44:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
24	20-abr-2017	6:46:00 PM	6:51:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
25	20-abr-2017	6:53:00 PM	6:58:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
26	20-abr-2017	7:00:00 PM	7:05:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
27	20-abr-2017	7:10:00 PM	7:15:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
28	20-abr-2017	7:22:00 PM	7:27:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
29	20-abr-2017	7:29:00 PM	7:34:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
30	20-abr-2017	7:38:00 PM	7:43:00 PM	0:05:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
31	22-abr-2017	9:03:00 AM	9:08:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
32	22-abr-2017	9:11:00 AM	9:16:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
33	22-abr-2017	9:19:00 AM	9:24:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
34	22-abr-2017	9:26:00 AM	9:31:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
35	22-abr-2017	9:34:00 AM	9:39:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
36	22-abr-2017	9:42:00 AM	9:47:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
37	22-abr-2017	9:50:00 AM	9:55:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
38	22-abr-2017	9:57:00 AM	10:02:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
39	22-abr-2017	10:04:00 AM	10:09:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
40	22-abr-2017	10:11:00 AM	10:16:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
41	22-abr-2017	10:18:00 AM	10:23:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
42	22-abr-2017	10:25:00 AM	10:30:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
43	22-abr-2017	10:32:00 AM	10:37:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
44	22-abr-2017	10:40:00 AM	10:45:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
45	22-abr-2017	10:47:00 AM	10:52:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
46	22-abr-2017	10:55:00 AM	11:00:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
47	22-abr-2017	11:02:00 AM	11:07:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
48	22-abr-2017	11:09:00 AM	11:14:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
49	22-abr-2017	11:16:00 AM	11:21:00 AM	0:05:00	190.239.151.190/192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100%
50	12-jun-2017	7:16:00 PM	7:21:00 PM	0:05:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (10 MINUTOS)**

	Abril/Mayo	Periodo de Tiempo (10')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	21-abr-2017	9:47:02 AM	9:57:02 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
2	21-abr-2017	10:10:04 AM	10:20:04 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
3	21-abr-2017	10:36:03 AM	10:46:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
4	21-abr-2017	11:04:03 AM	11:14:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
5	21-abr-2017	12:07:02 PM	12:17:02 PM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
6	24-abr-2017	10:08:01 AM	10:18:01 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
7	24-abr-2017	10:33:03 AM	10:43:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
8	24-abr-2017	11:14:04 AM	11:24:04 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
9	24-abr-2017	11:36:11 AM	11:46:11 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
10	24-abr-2017	12:04:05 PM	12:14:05 PM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	0	0,00%	100,00%
11	8-may-2017	9:33:00 AM	9:43:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
12	8-may-2017	10:03:00 AM	10:13:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	11	22,00%	78,00%
13	8-may-2017	10:33:00 AM	10:43:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	31	62,00%	38,00%
14	8-may-2017	10:52:00 AM	11:02:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	29	58,00%	42,00%
15	8-may-2017	11:14:00 AM	11:24:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
16	8-may-2017	11:29:00 AM	11:39:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	29	58,00%	42,00%
17	8-may-2017	11:44:00 AM	11:54:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
18	8-may-2017	4:24:00 PM	4:34:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
19	8-may-2017	4:37:00 PM	4:47:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
20	8-may-2017	4:49:00 PM	4:59:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	28	56,00%	44,00%
21	8-may-2017	5:21:00 PM	5:31:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
22	8-may-2017	5:34:00 PM	5:44:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
23	8-may-2017	5:50:05 PM	6:00:05 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
24	8-may-2017	6:07:00 PM	6:17:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
25	8-may-2017	6:21:00 PM	6:31:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
26	9-may-2017	9:14:00 AM	9:24:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
27	9-may-2017	9:35:00 AM	9:45:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
28	9-may-2017	9:48:00 AM	9:58:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
29	9-may-2017	10:03:00 AM	10:13:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
30	9-may-2017	10:18:00 AM	10:28:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
31	9-may-2017	10:31:00 AM	10:41:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
32	9-may-2017	10:44:00 AM	10:54:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
33	9-may-2017	11:00:00 AM	11:10:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
34	9-may-2017	11:12:00 AM	11:22:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
35	9-may-2017	11:30:00 AM	11:40:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
36	9-may-2017	11:42:00 AM	11:52:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
37	9-may-2017	11:55:00 AM	12:05:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
38	9-may-2017	12:08:00 PM	12:18:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
39	9-may-2017	12:20:00 PM	12:30:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
40	9-may-2017	12:35:00 PM	12:45:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
41	9-may-2017	12:50:00 PM	1:00:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
42	9-may-2017	1:03:00 PM	1:13:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
43	9-may-2017	1:18:00 PM	1:28:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
44	9-may-2017	1:35:00 PM	1:45:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
45	9-may-2017	1:50:00 PM	2:00:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
46	9-may-2017	4:04:00 PM	4:14:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	29	58,00%	42,00%
47	9-may-2017	4:20:00 PM	4:30:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
48	9-may-2017	4:33:00 PM	4:43:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
49	9-may-2017	4:47:00 PM	4:57:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
50	12-jun-2017	6:53:00 PM	7:03:00 PM	0:10:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
									PROMEDIO	20,68%	79,32%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (10 MINUTOS)**

	Abril/Mayo	Periodo de Tiempo (10')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	21-abr-2017	9:47:02 AM	9:57:02 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
2	21-abr-2017	10:10:04 AM	10:20:04 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
3	21-abr-2017	10:36:03 AM	10:46:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
4	21-abr-2017	11:04:03 AM	11:14:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
5	21-abr-2017	12:07:02 PM	12:17:02 PM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
6	24-abr-2017	10:08:01 AM	10:18:01 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
7	24-abr-2017	10:33:03 AM	10:43:03 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
8	24-abr-2017	11:14:04 AM	11:24:04 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
9	24-abr-2017	11:36:11 AM	11:46:11 AM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
10	24-abr-2017	12:04:05 PM	12:14:05 PM	0:10:00	190.233.71.176 / 192.168.1.24	Activo	181.66.25.13	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
11	8-may-2017	9:33:00 AM	9:43:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
12	8-may-2017	10:03:00 AM	10:13:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
13	8-may-2017	10:33:00 AM	10:43:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
14	8-may-2017	10:52:00 AM	11:02:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
15	8-may-2017	11:14:00 AM	11:24:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
16	8-may-2017	11:29:00 AM	11:39:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
17	8-may-2017	11:44:00 AM	11:54:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
18	8-may-2017	4:24:00 PM	4:34:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
19	8-may-2017	4:37:00 PM	4:47:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
20	8-may-2017	4:49:00 PM	4:59:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
21	8-may-2017	5:21:00 PM	5:31:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
22	8-may-2017	5:34:00 PM	5:44:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
23	8-may-2017	5:50:05 PM	6:00:05 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
24	8-may-2017	6:07:00 PM	6:17:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
25	8-may-2017	6:21:00 PM	6:31:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
26	9-may-2017	9:14:00 AM	9:24:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
27	9-may-2017	9:35:00 AM	9:45:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
28	9-may-2017	9:48:00 AM	9:58:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
29	9-may-2017	10:03:00 AM	10:13:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
30	9-may-2017	10:18:00 AM	10:28:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
31	9-may-2017	10:31:00 AM	10:41:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
32	9-may-2017	10:44:00 AM	10:54:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
33	9-may-2017	11:00:00 AM	11:10:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
34	9-may-2017	11:12:00 AM	11:22:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
35	9-may-2017	11:30:00 AM	11:40:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
36	9-may-2017	11:42:00 AM	11:52:00 AM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
37	9-may-2017	11:55:00 AM	12:05:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
38	9-may-2017	12:08:00 PM	12:18:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
39	9-may-2017	12:20:00 PM	12:30:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
40	9-may-2017	12:35:00 PM	12:45:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
41	9-may-2017	12:50:00 PM	1:00:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
42	9-may-2017	1:03:00 PM	1:13:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
43	9-may-2017	1:18:00 PM	1:28:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
44	9-may-2017	1:35:00 PM	1:45:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
45	9-may-2017	1:50:00 PM	2:00:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
46	9-may-2017	4:04:00 PM	4:14:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
47	9-may-2017	4:20:00 PM	4:30:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
48	9-may-2017	4:33:00 PM	4:43:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
49	9-may-2017	4:47:00 PM	4:57:00 PM	0:10:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.134.88	50	0	0,00%	100,00%
50	12-jun-2017	6:53:00 PM	7:03:00 PM	0:10:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (15 MINUTOS)**

	Mayo	Periodo de Tiempo (15')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	10-may-2017	9:15:00 AM	9:30:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
2	10-may-2017	9:38:00 AM	9:53:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
3	10-may-2017	10:15:00 AM	10:30:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
4	10-may-2017	10:34:00 AM	10:49:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
5	10-may-2017	10:53:00 AM	11:08:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	1	2,00%	98,00%
6	10-may-2017	11:14:00 AM	11:29:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
7	10-may-2017	11:34:00 AM	11:49:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
8	10-may-2017	11:55:00 AM	12:10:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
9	10-may-2017	12:15:00 PM	12:30:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	30	60,00%	40,00%
10	10-may-2017	12:37:00 PM	12:52:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	0	0,00%	100,00%
11	12-may-2017	9:18:00 AM	9:33:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	35	70,00%	30,00%
12	12-may-2017	9:48:00 AM	10:03:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	30	60,00%	40,00%
13	12-may-2017	10:08:00 AM	10:23:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	5	10,00%	90,00%
14	12-may-2017	10:37:00 AM	10:52:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	22	44,00%	56,00%
15	12-may-2017	10:57:00 AM	11:12:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	28	56,00%	44,00%
16	12-may-2017	11:18:00 AM	11:33:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	23	46,00%	54,00%
17	15-may-2017	9:39:00 AM	9:54:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	29	58,00%	42,00%
18	15-may-2017	10:02:00 AM	10:17:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	17	34,00%	66,00%
19	15-may-2017	10:20:00 AM	10:35:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	22	44,00%	56,00%
20	15-may-2017	10:43:00 AM	10:58:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	0	0,00%	100,00%
21	15-may-2017	11:04:00 AM	11:19:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	0	0,00%	100,00%
22	15-may-2017	11:35:00 AM	11:50:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	0	0,00%	100,00%
23	15-may-2017	11:54:00 AM	12:09:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	1	2,00%	98,00%
24	15-may-2017	12:13:00 PM	12:28:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	0	0,00%	100,00%
25	15-may-2017	12:33:00 PM	12:48:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	30	60,00%	40,00%
26	15-may-2017	1:01:00 PM	1:16:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	0	0,00%	100,00%
27	15-may-2017	1:20:00 PM	1:35:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	0	0,00%	100,00%
28	15-may-2017	1:37:00 PM	1:52:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	0	0,00%	100,00%
29	15-may-2017	1:55:00 PM	2:10:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	1	2,00%	98,00%
30	15-may-2017	2:13:00 PM	2:28:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	0	0,00%	100,00%
31	15-may-2017	2:30:00 PM	2:45:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	30	60,00%	40,00%
32	15-may-2017	4:05:00 PM	4:20:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	30	60,00%	40,00%
33	15-may-2017	4:22:00 PM	4:37:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
34	15-may-2017	4:40:00 PM	4:55:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
35	15-may-2017	4:58:00 PM	5:13:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
36	15-may-2017	5:15:00 PM	5:30:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
37	15-may-2017	5:33:00 PM	5:48:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
38	15-may-2017	5:50:00 PM	6:05:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
39	15-may-2017	6:08:00 PM	6:23:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	30	60,00%	40,00%
40	15-may-2017	6:26:00 PM	6:41:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
41	15-may-2017	6:45:00 PM	7:00:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
42	15-may-2017	7:02:00 PM	7:17:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
43	15-may-2017	7:20:00 PM	7:35:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	30	60,00%	40,00%
44	15-may-2017	7:37:00 PM	7:52:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
45	15-may-2017	7:55:00 PM	8:10:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
46	15-may-2017	8:12:00 PM	8:27:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
47	15-may-2017	8:30:00 PM	8:45:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
48	15-may-2017	8:47:00 PM	9:02:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
49	15-may-2017	9:05:00 PM	9:20:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	0	0,00%	100,00%
50	12-jun-2017	6:19:00 PM	6:34:00 PM	0:15:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
									PROMEDIO	22,96%	77,04%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (15 MINUTOS)**

	Mayo	Periodo de Tiempo (15')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	10-may-2017	9:15:00 AM	9:30:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
2	10-may-2017	9:38:00 AM	9:53:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
3	10-may-2017	10:15:00 AM	10:30:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
4	10-may-2017	10:34:00 AM	10:49:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
5	10-may-2017	10:53:00 AM	11:08:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
6	10-may-2017	11:14:00 AM	11:29:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
7	10-may-2017	11:34:00 AM	11:49:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
8	10-may-2017	11:55:00 AM	12:10:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
9	10-may-2017	12:15:00 PM	12:30:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
10	10-may-2017	12:37:00 PM	12:52:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.63.231	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
11	12-may-2017	9:18:00 AM	9:33:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
12	12-may-2017	9:48:00 AM	10:03:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
13	12-may-2017	10:08:00 AM	10:23:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
14	12-may-2017	10:37:00 AM	10:52:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
15	12-may-2017	10:57:00 AM	11:12:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
16	12-may-2017	11:18:00 AM	11:33:00 AM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
17	15-may-2017	9:39:00 AM	9:54:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
18	15-may-2017	10:02:00 AM	10:17:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.133.165	50	0	0,00%	100,00%
19	15-may-2017	10:20:00 AM	10:35:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
20	15-may-2017	10:43:00 AM	10:58:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
21	15-may-2017	11:04:00 AM	11:19:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
22	15-may-2017	11:35:00 AM	11:50:00 AM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
23	15-may-2017	11:54:00 AM	12:09:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
24	15-may-2017	12:13:00 PM	12:28:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
25	15-may-2017	12:33:00 PM	12:48:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
26	15-may-2017	1:01:00 PM	1:16:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
27	15-may-2017	1:20:00 PM	1:35:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
28	15-may-2017	1:37:00 PM	1:52:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,42,157,94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
29	15-may-2017	1:55:00 PM	2:10:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
30	15-may-2017	2:13:00 PM	2:28:00 PM	0:15:00	190.236.175.44 / 192.168.1.24	Activo	190,236,175,207	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
31	15-may-2017	2:30:00 PM	2:45:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
32	15-may-2017	4:05:00 PM	4:20:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
33	15-may-2017	4:22:00 PM	4:37:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
34	15-may-2017	4:40:00 PM	4:55:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
35	15-may-2017	4:58:00 PM	5:13:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
36	15-may-2017	5:15:00 PM	5:30:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
37	15-may-2017	5:33:00 PM	5:48:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
38	15-may-2017	5:50:00 PM	6:05:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
39	15-may-2017	6:08:00 PM	6:23:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
40	15-may-2017	6:26:00 PM	6:41:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
41	15-may-2017	6:45:00 PM	7:00:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
42	15-may-2017	7:02:00 PM	7:17:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
43	15-may-2017	7:20:00 PM	7:35:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
44	15-may-2017	7:37:00 PM	7:52:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
45	15-may-2017	7:55:00 PM	8:10:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
46	15-may-2017	8:12:00 PM	8:27:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
47	15-may-2017	8:30:00 PM	8:45:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
48	15-may-2017	8:47:00 PM	9:02:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
49	15-may-2017	9:05:00 PM	9:20:00 PM	0:15:00	190.235.51.95 / 192.168.1.24	Activo	190.233.72,99	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
50	12-jun-2017	6:19:00 PM	6:34:00 PM	0:15:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (20 MINUTOS)**

	Mayo	Periodo de Tiempo (20')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	16-may-2017	9:49:00 AM	10:09:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	0	0,00%	100,00%
2	16-may-2017	10:12:00 AM	10:32:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	29	58,00%	42,00%
3	16-may-2017	10:39:00 AM	10:59:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	0	0,00%	100,00%
4	16-may-2017	11:08:00 AM	11:28:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	6	12,00%	88,00%
5	16-may-2017	11:31:00 AM	11:51:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	0	0,00%	100,00%
6	16-may-2017	12:04:00 PM	12:24:00 PM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	0	0,00%	100,00%
7	16-may-2017	12:28:00 PM	12:48:00 PM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	0	0,00%	100,00%
8	17-may-2017	9:41:00 AM	10:01:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	30	60,00%	40,00%
9	17-may-2017	10:09:00 AM	10:29:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	0	0,00%	100,00%
10	17-may-2017	10:33:00 AM	10:53:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	23	46,00%	54,00%
11	17-may-2017	10:59:00 AM	11:19:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	0	0,00%	100,00%
12	17-may-2017	11:23:00 AM	11:43:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	9	18,00%	82,00%
13	17-may-2017	11:49:00 AM	12:09:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	0	0,00%	100,00%
14	17-may-2017	12:16:00 PM	12:36:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	0	0,00%	100,00%
15	17-may-2017	12:39:00 PM	12:59:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	4	8,00%	92,00%
16	18-may-2017	9:21:00 AM	9:41:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	30	60,00%	40,00%
17	18-may-2017	9:46:00 AM	10:06:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	30	60,00%	40,00%
18	18-may-2017	10:10:00 AM	10:30:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	0	0,00%	100,00%
19	18-may-2017	10:34:00 AM	10:54:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	0	0,00%	100,00%
20	18-may-2017	11:15:00 AM	11:35:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	190.42.227.131	Denegado/Anomalía	0	0,00%	100,00%
21	19-may-2017	9:18:00 AM	9:38:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
22	19-may-2017	9:42:00 AM	10:02:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	19	38,00%	62,00%
23	19-may-2017	10:06:00 AM	10:26:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
24	19-may-2017	10:29:00 AM	10:49:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
25	19-may-2017	10:54:00 AM	11:14:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	29	58,00%	42,00%
26	19-may-2017	11:22:00 AM	11:42:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
27	19-may-2017	11:55:00 AM	12:15:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	18	36,00%	64,00%
28	19-may-2017	12:23:00 PM	12:43:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	2	4,00%	96,00%
29	19-may-2017	12:52:00 PM	1:12:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	12	24,00%	76,00%
30	19-may-2017	1:15:00 PM	1:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	2	4,00%	96,00%
31	19-may-2017	1:40:00 PM	2:00:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
32	19-may-2017	4:02:00 PM	4:12:00 PM	0:10:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
33	19-may-2017	4:15:00 PM	4:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
34	19-may-2017	4:39:00 PM	4:59:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
35	19-may-2017	5:03:00 PM	5:23:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
36	19-may-2017	5:29:00 PM	5:49:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
37	19-may-2017	5:52:00 PM	6:12:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
38	19-may-2017	6:15:00 PM	6:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	29	58,00%	42,00%
39	19-may-2017	6:40:00 PM	7:00:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
40	19-may-2017	7:04:00 PM	7:24:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
41	19-may-2017	7:30:00 PM	7:50:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
42	19-may-2017	7:55:00 PM	8:15:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
43	20-may-2017	9:04:00 AM	9:24:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
44	20-may-2017	9:26:00 AM	9:46:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
45	20-may-2017	9:50:00 AM	10:10:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
46	20-may-2017	10:20:00 AM	10:40:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	0	0,00%	100,00%
47	20-may-2017	10:44:00 AM	11:04:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
48	20-may-2017	11:09:00 AM	11:29:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
49	20-may-2017	11:34:00 AM	11:54:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	30	60,00%	40,00%
50	24-may-2017	10:13:00 AM	10:33:00 AM	0:20:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	30	60,00%	40,00%
									PROMEDIO	24,08%	75,92%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (20 MINUTOS)**

	Mayo	Periodo de Tiempo (20')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	16-may-2017	9:49:00 AM	10:09:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
2	16-may-2017	10:12:00 AM	10:32:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
3	16-may-2017	10:39:00 AM	10:59:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
4	16-may-2017	11:08:00 AM	11:28:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
5	16-may-2017	11:31:00 AM	11:51:00 AM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
6	16-may-2017	12:04:00 PM	12:24:00 PM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
7	16-may-2017	12:28:00 PM	12:48:00 PM	0:20:00	190.42.239.202 / 192.168.1.24	Activo	190.42.157.94	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
8	17-may-2017	9:41:00 AM	10:01:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
9	17-may-2017	10:09:00 AM	10:29:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
10	17-may-2017	10:33:00 AM	10:53:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
11	17-may-2017	10:59:00 AM	11:19:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
12	17-may-2017	11:23:00 AM	11:43:00 AM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
13	17-may-2017	11:49:00 AM	12:09:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
14	17-may-2017	12:16:00 PM	12:36:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
15	17-may-2017	12:39:00 PM	12:59:00 PM	0:20:00	190.233.67.132 / 192.168.1.24	Activo	181.66.204.236	Denegado/Anomalía	179.7.138.173	50	0	0,00%	100,00%
16	18-may-2017	9:21:00 AM	9:41:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
17	18-may-2017	9:46:00 AM	10:06:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
18	18-may-2017	10:10:00 AM	10:30:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	179.7.137.237	48	2	4,00%	96,00%
19	18-may-2017	10:34:00 AM	10:54:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	181.65.37.217	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
20	18-may-2017	11:15:00 AM	11:35:00 AM	0:20:00	190.233.73.159 / 192.168.1.24	Activo	190.42.227.131	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
21	19-may-2017	9:18:00 AM	9:38:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
22	19-may-2017	9:42:00 AM	10:02:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
23	19-may-2017	10:06:00 AM	10:26:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
24	19-may-2017	10:29:00 AM	10:49:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
25	19-may-2017	10:54:00 AM	11:14:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
26	19-may-2017	11:22:00 AM	11:42:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
27	19-may-2017	11:55:00 AM	12:15:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
28	19-may-2017	12:23:00 PM	12:43:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
29	19-may-2017	12:52:00 PM	1:12:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
30	19-may-2017	1:15:00 PM	1:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
31	19-may-2017	1:40:00 PM	2:00:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
32	19-may-2017	4:02:00 PM	4:12:00 PM	0:10:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
33	19-may-2017	4:15:00 PM	4:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
34	19-may-2017	4:39:00 PM	4:59:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
35	19-may-2017	5:03:00 PM	5:23:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
36	19-may-2017	5:29:00 PM	5:49:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
37	19-may-2017	5:52:00 PM	6:12:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
38	19-may-2017	6:15:00 PM	6:35:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
39	19-may-2017	6:40:00 PM	7:00:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
40	19-may-2017	7:04:00 PM	7:24:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
41	19-may-2017	7:30:00 PM	7:50:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
42	19-may-2017	7:55:00 PM	8:15:00 PM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
43	20-may-2017	9:04:00 AM	9:24:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
44	20-may-2017	9:26:00 AM	9:46:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
45	20-may-2017	9:50:00 AM	10:10:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
46	20-may-2017	10:20:00 AM	10:40:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
47	20-may-2017	10:44:00 AM	11:04:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
48	20-may-2017	11:09:00 AM	11:29:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
49	20-may-2017	11:34:00 AM	11:54:00 AM	0:20:00	190.233.63.18 / 192.168.1.24	Activo	201.240.30.204	Denegado/Anomalía	179.7.137.237	50	0	0,00%	100,00%
50	24-may-2017	10:13:00 AM	10:33:00 AM	0:20:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100,00%
											PROMEDIO	0,08%	99,92%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (25 MINUTOS)**

	Mayo	Periodo de Tiempo (25')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	23-may-2017	10:17:00 AM	10:42:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	30	60,00%	40,00%
2	23-may-2017	10:46:00 AM	11:11:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	29	58,00%	42,00%
3	23-may-2017	11:19:00 AM	11:44:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	30	60,00%	40,00%
4	23-may-2017	11:48:00 AM	12:13:00 PM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	30	60,00%	40,00%
5	23-may-2017	12:18:00 PM	12:43:00 PM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	30	60,00%	40,00%
6	26-may-2017	9:53:00 AM	10:18:00 AM	0:25:00	190.233.67.104 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	30	60,00%	40,00%
7	26-may-2017	10:22:00 AM	10:47:00 AM	0:25:00	190.233.67.104 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	29	58,00%	42,00%
8	29-may-2017	9:50:00 AM	10:15:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	30	60,00%	40,00%
9	29-may-2017	10:22:00 AM	10:47:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	30	60,00%	40,00%
10	29-may-2017	10:51:00 AM	11:16:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	30	60,00%	40,00%
11	29-may-2017	11:21:00 AM	11:46:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	0	0,00%	100,00%
12	29-may-2017	11:52:00 AM	12:17:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	0	0,00%	100,00%
13	29-may-2017	12:21:00 PM	12:46:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	30	60,00%	40,00%
14	29-may-2017	12:52:00 PM	1:17:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	0	0,00%	100,00%
15	29-may-2017	1:22:00 PM	1:47:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	24	48,00%	52,00%
16	30-may-2017	9:42:00 AM	10:07:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	28	56,00%	44,00%
17	31-may-2017	9:58:00 AM	10:23:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	30	60,00%	40,00%
18	31-may-2017	10:30:00 AM	10:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	18	36,00%	64,00%
19	31-may-2017	11:00:00 AM	11:25:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	9	18,00%	82,00%
20	31-may-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	24	48,00%	52,00%
21	31-may-2017	4:35:00 PM	5:00:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	30	60,00%	40,00%
22	31-may-2017	5:04:00 PM	5:29:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	26	52,00%	48,00%
23	31-may-2017	5:38:00 PM	6:03:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	0	0,00%	100,00%
24	1-jun-2017	10:18:00 AM	10:43:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	5	10,00%	90,00%
25	1-jun-2017	10:53:00 AM	11:18:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	13	26,00%	74,00%
26	1-jun-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	10	20,00%	80,00%
27	1-jun-2017	12:02:00 PM	12:27:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	7	14,00%	86,00%
28	1-jun-2017	12:35:00 PM	1:00:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	10	20,00%	80,00%
29	1-jun-2017	1:05:00 PM	1:30:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
30	1-jun-2017	1:40:00 PM	2:05:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	2	4,00%	96,00%
31	1-jun-2017	2:10:00 PM	2:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
32	1-jun-2017	4:01:00 PM	4:26:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	1	2,00%	98,00%
33	1-jun-2017	4:30:00 PM	4:55:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
34	1-jun-2017	5:10:00 PM	5:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
35	1-jun-2017	5:42:00 PM	6:07:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
36	1-jun-2017	6:18:00 PM	6:43:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
37	1-jun-2017	6:55:00 PM	7:20:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
38	1-jun-2017	7:26:00 PM	7:51:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
39	1-jun-2017	8:00:00 PM	8:25:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
40	1-jun-2017	8:32:00 PM	8:57:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
41	1-jun-2017	9:12:00 PM	9:37:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
42	2-jun-2017	9:15:00 AM	9:40:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
43	2-jun-2017	9:51:00 AM	10:16:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	29	58,00%	42,00%
44	2-jun-2017	10:25:00 AM	10:50:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
45	2-jun-2017	11:00:00 AM	11:25:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	0	0,00%	100,00%
46	2-jun-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
47	2-jun-2017	12:10:00 PM	12:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	30	60,00%	40,00%
48	5-jun-2017	9:16:00 AM	9:41:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
49	5-jun-2017	9:55:00 AM	10:20:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
50	12-jun-2017	5:37:00 PM	6:02:00 PM	0:25:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
									PROMEDIO	33,36%	66,64%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (25 MINUTOS)**

	Mayo	Periodo de Tiempo (25')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	23-may-2017	10:17:00 AM	10:42:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100%
2	23-may-2017	10:46:00 AM	11:11:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100%
3	23-may-2017	11:19:00 AM	11:44:00 AM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100%
4	23-may-2017	11:48:00 AM	12:13:00 PM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100%
5	23-may-2017	12:18:00 PM	12:43:00 PM	0:25:00	201.240.174.145 / 192.168.1.24	Activo	181.67.151.115	Denegado/Anomalía	179.7.132.74	50	0	0,00%	100%
6	26-may-2017	9:53:00 AM	10:18:00 AM	0:25:00	190.233.67.104 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
7	26-may-2017	10:22:00 AM	10:47:00 AM	0:25:00	190.233.67.104 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
8	29-may-2017	9:50:00 AM	10:15:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
9	29-may-2017	10:22:00 AM	10:47:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
10	29-may-2017	10:51:00 AM	11:16:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
11	29-may-2017	11:21:00 AM	11:46:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
12	29-may-2017	11:52:00 AM	12:17:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
13	29-may-2017	12:21:00 PM	12:46:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
14	29-may-2017	12:52:00 PM	1:17:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
15	29-may-2017	1:22:00 PM	1:47:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
16	30-may-2017	9:42:00 AM	10:07:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.229	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
17	31-may-2017	9:58:00 AM	10:23:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
18	31-may-2017	10:30:00 AM	10:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
19	31-may-2017	11:00:00 AM	11:25:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
20	31-may-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
21	31-may-2017	4:35:00 PM	5:00:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
22	31-may-2017	5:04:00 PM	5:29:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
23	31-may-2017	5:38:00 PM	6:03:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.233.190	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
24	1-jun-2017	10:18:00 AM	10:43:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
25	1-jun-2017	10:53:00 AM	11:18:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
26	1-jun-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
27	1-jun-2017	12:02:00 PM	12:27:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
28	1-jun-2017	12:35:00 PM	1:00:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.111	50	0	0,00%	100%
29	1-jun-2017	1:05:00 PM	1:30:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
30	1-jun-2017	1:40:00 PM	2:05:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
31	1-jun-2017	2:10:00 PM	2:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
32	1-jun-2017	4:01:00 PM	4:26:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
33	1-jun-2017	4:30:00 PM	4:55:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
34	1-jun-2017	5:10:00 PM	5:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
35	1-jun-2017	5:42:00 PM	6:07:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
36	1-jun-2017	6:18:00 PM	6:43:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
37	1-jun-2017	6:55:00 PM	7:20:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
38	1-jun-2017	7:26:00 PM	7:51:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
39	1-jun-2017	8:00:00 PM	8:25:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
40	1-jun-2017	8:32:00 PM	8:57:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
41	1-jun-2017	9:12:00 PM	9:37:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
42	2-jun-2017	9:15:00 AM	9:40:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
43	2-jun-2017	9:51:00 AM	10:16:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
44	2-jun-2017	10:25:00 AM	10:50:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
45	2-jun-2017	11:00:00 AM	11:25:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
46	2-jun-2017	11:30:00 AM	11:55:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
47	2-jun-2017	12:10:00 PM	12:35:00 PM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.233.86.47	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
48	5-jun-2017	9:16:00 AM	9:41:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
49	5-jun-2017	9:55:00 AM	10:20:00 AM	0:25:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100%
50	12-jun-2017	5:37:00 PM	6:02:00 PM	0:25:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (30 MINUTOS)**

	Mayo	Periodo de Tiempo (30')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	5-jun-2017	10:40:00 AM	11:10:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
2	5-jun-2017	11:14:00 AM	11:44:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
3	5-jun-2017	11:50:00 AM	12:20:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
4	5-jun-2017	12:28:00 PM	12:58:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
5	5-jun-2017	4:54:00 PM	5:24:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	29	58,00%	42,00%
6	5-jun-2017	5:30:00 PM	6:00:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
7	5-jun-2017	6:08:00 PM	6:38:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
8	6-jun-2017	9:14:00 AM	9:44:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
9	6-jun-2017	9:49:00 AM	10:19:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
10	6-jun-2017	10:24:00 AM	10:54:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
11	6-jun-2017	11:01:00 AM	11:31:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
12	6-jun-2017	11:36:00 AM	12:06:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
13	7-jun-2017	9:17:00 AM	9:47:00 AM	0:30:00	190.233.78.9 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
14	7-jun-2017	10:02:00 AM	10:32:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
15	7-jun-2017	10:38:00 AM	11:08:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
16	7-jun-2017	11:13:00 AM	11:43:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
17	7-jun-2017	12:01:00 PM	12:31:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
18	7-jun-2017	4:40:00 PM	5:10:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
19	7-jun-2017	5:15:00 PM	5:45:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
20	7-jun-2017	5:49:00 PM	6:19:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
21	8-jun-2017	8:56:00 AM	9:26:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
22	8-jun-2017	9:32:00 AM	10:02:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
23	8-jun-2017	10:07:00 AM	10:37:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	29	58,00%	42,00%
24	8-jun-2017	10:46:00 AM	11:16:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
25	8-jun-2017	11:21:00 AM	11:51:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	39	78,00%	22,00%
26	8-jun-2017	12:04:00 PM	12:34:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
27	9-jun-2017	9:02:00 AM	9:32:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
28	9-jun-2017	9:36:00 AM	10:06:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
29	9-jun-2017	10:12:00 AM	10:42:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
30	9-jun-2017	10:51:00 AM	11:21:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
31	9-jun-2017	11:32:00 AM	12:02:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
32	9-jun-2017	12:15:00 PM	12:45:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
33	9-jun-2017	12:57:00 PM	1:27:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
34	9-jun-2017	1:39:00 PM	2:09:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
35	9-jun-2017	4:04:00 PM	4:34:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
36	9-jun-2017	4:42:00 PM	5:12:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
37	9-jun-2017	5:20:00 PM	5:50:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
38	9-jun-2017	5:56:00 PM	6:26:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
39	9-jun-2017	6:33:00 PM	7:03:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
40	9-jun-2017	7:10:00 PM	7:40:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
41	9-jun-2017	7:49:00 PM	8:19:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
42	9-jun-2017	8:26:00 PM	8:56:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
43	9-jun-2017	9:07:00 PM	9:37:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
44	9-jun-2017	9:45:00 PM	10:15:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	0	0,00%	100,00%
45	9-jun-2017	10:23:00 PM	10:53:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	30	60,00%	40,00%
46	12-jun-2017	9:38:00 AM	10:08:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
47	12-jun-2017	10:11:00 AM	10:41:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
48	12-jun-2017	10:44:00 AM	11:14:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
49	12-jun-2017	11:17:00 AM	11:47:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
50	12-jun-2017	4:42:00 PM	5:12:00 PM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	26	52,00%	48,00%
									PROMEDIO	33,72%	66,28%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (30 MINUTOS)**

	Mayo	Periodo de Tiempo (30')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	5-jun-2017	10:40:00 AM	11:10:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
2	5-jun-2017	11:14:00 AM	11:44:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
3	5-jun-2017	11:50:00 AM	12:20:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
4	5-jun-2017	12:28:00 PM	12:58:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
5	5-jun-2017	4:54:00 PM	5:24:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
6	5-jun-2017	5:30:00 PM	6:00:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
7	5-jun-2017	6:08:00 PM	6:38:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
8	6-jun-2017	9:14:00 AM	9:44:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
9	6-jun-2017	9:49:00 AM	10:19:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
10	6-jun-2017	10:24:00 AM	10:54:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
11	6-jun-2017	11:01:00 AM	11:31:00 AM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
12	6-jun-2017	11:36:00 AM	12:06:00 PM	0:30:00	181.64.23.125 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
13	7-jun-2017	9:17:00 AM	9:47:00 AM	0:30:00	190.233.78.9 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
14	7-jun-2017	10:02:00 AM	10:32:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
15	7-jun-2017	10:38:00 AM	11:08:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
16	7-jun-2017	11:13:00 AM	11:43:00 AM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
17	7-jun-2017	12:01:00 PM	12:31:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
18	7-jun-2017	4:40:00 PM	5:10:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
19	7-jun-2017	5:15:00 PM	5:45:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
20	7-jun-2017	5:49:00 PM	6:19:00 PM	0:30:00	181.65.83.239 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.135.47	50	0	0,00%	100,00%
21	8-jun-2017	8:56:00 AM	9:26:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
22	8-jun-2017	9:32:00 AM	10:02:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
23	8-jun-2017	10:07:00 AM	10:37:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
24	8-jun-2017	10:46:00 AM	11:16:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
25	8-jun-2017	11:21:00 AM	11:51:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
26	8-jun-2017	12:04:00 PM	12:34:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
27	9-jun-2017	9:02:00 AM	9:32:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
28	9-jun-2017	9:36:00 AM	10:06:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
29	9-jun-2017	10:12:00 AM	10:42:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
30	9-jun-2017	10:51:00 AM	11:21:00 AM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
31	9-jun-2017	11:32:00 AM	12:02:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
32	9-jun-2017	12:15:00 PM	12:45:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
33	9-jun-2017	12:57:00 PM	1:27:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
34	9-jun-2017	1:39:00 PM	2:09:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
35	9-jun-2017	4:04:00 PM	4:34:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
36	9-jun-2017	4:42:00 PM	5:12:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
37	9-jun-2017	5:20:00 PM	5:50:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
38	9-jun-2017	5:56:00 PM	6:26:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
39	9-jun-2017	6:33:00 PM	7:03:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
40	9-jun-2017	7:10:00 PM	7:40:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
41	9-jun-2017	7:49:00 PM	8:19:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
42	9-jun-2017	8:26:00 PM	8:56:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
43	9-jun-2017	9:07:00 PM	9:37:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
44	9-jun-2017	9:45:00 PM	10:15:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
45	9-jun-2017	10:23:00 PM	10:53:00 PM	0:30:00	181.66.34.139 / 192.168.1.24	Activo	190.42.157.40	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
46	12-jun-2017	9:38:00 AM	10:08:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
47	12-jun-2017	10:11:00 AM	10:41:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
48	12-jun-2017	10:44:00 AM	11:14:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
49	12-jun-2017	11:17:00 AM	11:47:00 AM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
50	12-jun-2017	4:42:00 PM	5:12:00 PM	0:30:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (60 MINUTOS)**

	Mayo	Periodo de Tiempo (60')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	13-jun-2017	9:04:00 AM	10:04:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
2	13-jun-2017	10:15:00 AM	11:15:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
3	13-jun-2017	11:21:00 AM	12:21:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
4	13-jun-2017	12:25:00 PM	1:25:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	0	0,00%	100,00%
5	14-jun-2017	9:28:00 AM	10:28:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	23	46,00%	54,00%
6	14-jun-2017	10:35:00 AM	11:35:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	30	60,00%	40,00%
7	19-jun-2017	8:49:00 AM	9:49:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
8	19-jun-2017	9:55:00 AM	10:55:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
9	19-jun-2017	11:00:00 AM	12:00:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	0	0,00%	100,00%
10	19-jun-2017	12:07:00 PM	1:07:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	0	0,00%	100,00%
11	20-jun-2017	9:39:00 AM	10:39:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
12	20-jun-2017	10:43:00 AM	11:43:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
13	20-jun-2017	11:57:00 AM	12:57:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	0	0,00%	100,00%
14	20-jun-2017	1:04:00 PM	2:04:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	1	2,00%	98,00%
15	21-jun-2017	9:01:00 AM	10:01:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
16	21-jun-2017	10:07:00 AM	11:07:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
17	21-jun-2017	11:18:00 AM	11:28:00 AM	0:10:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	8	16,00%	84,00%
18	21-jun-2017	12:22:00 PM	1:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
19	22-jun-2017	9:35:00 AM	10:35:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
20	22-jun-2017	10:41:00 AM	11:41:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
21	22-jun-2017	11:45:00 AM	12:45:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
22	23-jun-2017	9:22:00 AM	10:22:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	30	60,00%	40,00%
23	23-jun-2017	10:31:00 AM	11:31:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	0	0,00%	100,00%
24	23-jun-2017	11:41:00 AM	12:41:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	0	0,00%	100,00%
25	26-jul-2017	9:07:00 AM	10:07:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
26	26-jul-2017	10:46:00 AM	11:46:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
27	26-jul-2017	11:54:00 AM	12:54:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
28	27-jun-2017	9:27:00 AM	10:27:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
29	27-jun-2017	10:31:00 AM	11:31:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
30	27-jun-2017	11:37:00 AM	12:37:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
31	27-jun-2017	2:05:00 PM	3:05:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
32	27-jun-2017	3:11:00 PM	4:11:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
33	27-jun-2017	4:19:00 PM	5:19:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
34	27-jun-2017	5:22:00 PM	6:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
35	28-jun-2017	9:10:00 AM	10:10:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
36	28-jun-2017	10:15:00 AM	11:15:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
37	28-jun-2017	11:22:00 AM	12:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
38	28-jun-2017	12:30:00 PM	1:30:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
39	28-jun-2017	4:01:00 PM	5:01:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
40	28-jun-2017	5:09:00 PM	6:09:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
41	28-jun-2017	6:16:00 PM	7:16:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
42	29-jun-2017	8:52:00 AM	9:52:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
43	29-jun-2017	10:00:00 AM	11:00:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
44	29-jun-2017	11:15:00 AM	12:15:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
45	29-jun-2017	12:20:00 PM	1:20:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
46	30-jun-2017	8:45:00 AM	9:45:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
47	30-jun-2017	9:52:00 AM	10:52:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
48	30-jun-2017	10:59:00 AM	11:59:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
49	30-jun-2017	12:05:00 PM	1:05:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
50	9-ago-2017	10:47:00 AM	11:47:00 AM	1:00:00	190.233.84.59 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
									PROMEDIO	38,48%	61,52%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (60 MINUTOS)**

	Mayo	Periodo de Tiempo (60')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	13-jun-2017	9:04:00 AM	10:04:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
2	13-jun-2017	10:15:00 AM	11:15:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
3	13-jun-2017	11:21:00 AM	12:21:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
4	13-jun-2017	12:25:00 PM	1:25:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
5	14-jun-2017	9:28:00 AM	10:28:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
6	14-jun-2017	10:35:00 AM	11:35:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.67.151.240	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
7	19-jun-2017	8:49:00 AM	9:49:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
8	19-jun-2017	9:55:00 AM	10:55:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
9	19-jun-2017	11:00:00 AM	12:00:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
10	19-jun-2017	12:07:00 PM	1:07:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.134.35	50	0	0,00%	100,00%
11	20-jun-2017	9:39:00 AM	10:39:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
12	20-jun-2017	10:43:00 AM	11:43:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
13	20-jun-2017	11:57:00 AM	12:57:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
14	20-jun-2017	1:04:00 PM	2:04:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
15	21-jun-2017	9:01:00 AM	10:01:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
16	21-jun-2017	10:07:00 AM	11:07:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
17	21-jun-2017	11:18:00 AM	11:28:00 AM	0:10:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
18	21-jun-2017	12:22:00 PM	1:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
19	22-jun-2017	9:35:00 AM	10:35:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
20	22-jun-2017	10:41:00 AM	11:41:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
21	22-jun-2017	11:45:00 AM	12:45:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
22	23-jun-2017	9:22:00 AM	10:22:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
23	23-jun-2017	10:31:00 AM	11:31:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
24	23-jun-2017	11:41:00 AM	12:41:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	181.66.25.55	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
25	26-jul-2017	9:07:00 AM	10:07:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
26	26-jul-2017	10:46:00 AM	11:46:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
27	26-jul-2017	11:54:00 AM	12:54:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
28	27-jun-2017	9:27:00 AM	10:27:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
29	27-jun-2017	10:31:00 AM	11:31:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
30	27-jun-2017	11:37:00 AM	12:37:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
31	27-jun-2017	2:05:00 PM	3:05:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
32	27-jun-2017	3:11:00 PM	4:11:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
33	27-jun-2017	4:19:00 PM	5:19:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
34	27-jun-2017	5:22:00 PM	6:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
35	28-jun-2017	9:10:00 AM	10:10:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
36	28-jun-2017	10:15:00 AM	11:15:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
37	28-jun-2017	11:22:00 AM	12:22:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
38	28-jun-2017	12:30:00 PM	1:30:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
39	28-jun-2017	4:01:00 PM	5:01:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
40	28-jun-2017	5:09:00 PM	6:09:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
41	28-jun-2017	6:16:00 PM	7:16:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
42	29-jun-2017	8:52:00 AM	9:52:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
43	29-jun-2017	10:00:00 AM	11:00:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
44	29-jun-2017	11:15:00 AM	12:15:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
45	29-jun-2017	12:20:00 PM	1:20:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
46	30-jun-2017	8:45:00 AM	9:45:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
47	30-jun-2017	9:52:00 AM	10:52:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
48	30-jun-2017	10:59:00 AM	11:59:00 AM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
49	30-jun-2017	12:05:00 PM	1:05:00 PM	1:00:00	190.235.158.50 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
50	9-ago-2017	10:47:00 AM	11:47:00 AM	1:00:00	190.233.84.59 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	66.249.88.47	50	0	0,00%	100,00%
											PROMEDIO	0,00%	100,00%

- **FALSOS NEGATIVOS Y VERDADEROS POSITIVOS (90 MINUTOS)**

	Mayo	Periodo de Tiempo (90')					DETECCIÓN DE ATAQUES		FALSOS NEGATIVOS		VERDADEROS POSITIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	Numero de ataques no detectados	Tasa de FN	Tasa de VP
1	3-jul-2017	9:56:00 AM	11:26:00 AM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
2	3-jul-2017	11:35:00 AM	1:05:00 PM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	33	66,00%	34,00%
3	4-jul-2017	9:30:00 AM	11:00:00 AM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
4	4-jul-2017	11:09:00 AM	12:39:00 PM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
5	5-jul-2017	9:31:00 AM	11:01:00 AM	1:30:00	190.233.82.207 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
6	5-jul-2017	11:11:00 AM	12:41:00 PM	1:30:00	190.233.82.207 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
7	7-jul-2017	9:41:00 AM	11:11:00 AM	1:30:00	190.233.69.6 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
8	7-jul-2017	11:19:00 AM	12:49:00 PM	1:30:00	190.233.69.6 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
9	10-jul-2017	9:53:00 AM	11:23:00 AM	1:30:00	190.233.71.186 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
10	10-jul-2017	11:29:00 AM	12:59:00 PM	1:30:00	190.233.71.186 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
11	10-jul-2017	4:11:00 PM	5:41:00 PM	1:30:00	201.240.239.105 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
12	10-jul-2017	5:50:00 PM	7:20:00 PM	1:30:00	201.240.239.105 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
13	11-jul-2017	10:11:00 AM	11:41:00 AM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
14	11-jul-2017	11:44:00 AM	1:14:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
15	12-jul-2017	2:01:00 PM	3:31:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
16	12-jul-2017	3:37:00 PM	5:07:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
17	12-jul-2017	5:26:00 PM	6:56:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
18	14-jul-2017	9:00:00 AM	10:30:00 AM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
19	14-jul-2017	10:55:00 AM	12:25:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
20	14-jul-2017	12:42:00 PM	2:12:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
21	14-jul-2017	2:15:00 PM	3:45:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
22	18-jul-2017	9:22:00 AM	10:52:00 AM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
23	18-jul-2017	11:13:00 AM	12:43:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
24	18-jul-2017	12:51:00 PM	2:21:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
25	21-jul-2017	9:33:00 AM	11:03:00 AM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
26	21-jul-2017	11:09:00 AM	12:39:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
27	21-jul-2017	12:44:00 PM	2:14:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
28	24-jul-2017	1:11:00 PM	2:41:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
29	24-jul-2017	2:49:00 PM	4:19:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
30	24-jul-2017	4:25:00 PM	5:55:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
31	24-jul-2017	6:00:00 PM	7:30:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
32	25-jul-2017	2:05:00 PM	3:35:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
33	25-jul-2017	3:42:00 PM	5:12:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
34	25-jul-2017	5:20:00 PM	6:50:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
35	25-jul-2017	6:57:00 PM	8:27:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
36	26-jul-2017	8:53:00 AM	10:23:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
37	26-jul-2017	11:00:00 AM	12:30:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
38	26-jul-2017	2:23:00 PM	3:53:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
39	26-jul-2017	4:00:00 PM	5:30:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
40	26-jul-2017	5:38:00 PM	7:08:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
41	26-jul-2017	7:12:00 PM	8:42:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
42	27-jul-2017	9:02:00 AM	10:32:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
43	27-jul-2017	10:41:00 AM	12:11:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
44	27-jul-2017	3:02:00 PM	4:32:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
45	27-jul-2017	4:39:00 PM	6:09:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
46	28-jul-2017	9:05:00 AM	10:35:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	0	0,00%	100,00%
47	28-jul-2017	10:42:00 AM	12:12:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
48	28-jul-2017	2:06:00 PM	3:36:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
49	28-jul-2017	5:41:00 PM	7:11:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
50	9-ago-2017	10:01:00 AM	11:31:00 AM	1:30:00	190.235.51.28 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	30	60,00%	40,00%
									PROMEDIO	44,52%	55,48%

- **FALSOS POSITIVOS Y VERDADEROS NEGATIVOS (90 MINUTOS)**

	Mayo	Periodo de Tiempo (90')					DETECCIÓN DE ATAQUES		FALSOS POSITIVOS				VERDADEROS NEGATIVOS
Número de ataques	Fecha	Inicio de Ataque (Hora Inicial)	Seguimiento (Hora actual)	Duracion (H:M:S)	IP (Servidor) Pública/Privada	Acceso	IP PÚBLICA	Acceso/Tipo de tráfico	IP PUBLICA	Número de accesos positivos	Número de accesos fallidos	Tasa de FP	Tasa de VN
1	3-jul-2017	9:56:00 AM	11:26:00 AM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
2	3-jul-2017	11:35:00 AM	1:05:00 PM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
3	4-jul-2017	9:30:00 AM	11:00:00 AM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
4	4-jul-2017	11:09:00 AM	12:39:00 PM	1:30:00	190.42.233.242 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
5	5-jul-2017	9:31:00 AM	11:01:00 AM	1:30:00	190.233.82.207 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
6	5-jul-2017	11:11:00 AM	12:41:00 PM	1:30:00	190.233.82.207 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
7	7-jul-2017	9:41:00 AM	11:11:00 AM	1:30:00	190.233.69.6 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
8	7-jul-2017	11:19:00 AM	12:49:00 PM	1:30:00	190.233.69.6 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.138.161	50	0	0,00%	100,00%
9	10-jul-2017	9:53:00 AM	11:23:00 AM	1:30:00	190.233.71.186 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
10	10-jul-2017	11:29:00 AM	12:59:00 PM	1:30:00	190.233.71.186 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
11	10-jul-2017	4:11:00 PM	5:41:00 PM	1:30:00	201.240.239.105 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
12	10-jul-2017	5:50:00 PM	7:20:00 PM	1:30:00	201.240.239.105 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
13	11-jul-2017	10:11:00 AM	11:41:00 AM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
14	11-jul-2017	11:44:00 AM	1:14:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
15	12-jul-2017	2:01:00 PM	3:31:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
16	12-jul-2017	3:37:00 PM	5:07:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
17	12-jul-2017	5:26:00 PM	6:56:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
18	14-jul-2017	9:00:00 AM	10:30:00 AM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
19	14-jul-2017	10:55:00 AM	12:25:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
20	14-jul-2017	12:42:00 PM	2:12:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
21	14-jul-2017	2:15:00 PM	3:45:00 PM	1:30:00	190.233.62.78 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
22	18-jul-2017	9:22:00 AM	10:52:00 AM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
23	18-jul-2017	11:13:00 AM	12:43:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
24	18-jul-2017	12:51:00 PM	2:21:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.131.97	50	0	0,00%	100,00%
25	21-jul-2017	9:33:00 AM	11:03:00 AM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
26	21-jul-2017	11:09:00 AM	12:39:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
27	21-jul-2017	12:44:00 PM	2:14:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
28	24-jul-2017	1:11:00 PM	2:41:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
29	24-jul-2017	2:49:00 PM	4:19:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
30	24-jul-2017	4:25:00 PM	5:55:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
31	24-jul-2017	6:00:00 PM	7:30:00 PM	1:30:00	201.240.30.111 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.129.47	50	0	0,00%	100,00%
32	25-jul-2017	2:05:00 PM	3:35:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
33	25-jul-2017	3:42:00 PM	5:12:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
34	25-jul-2017	5:20:00 PM	6:50:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
35	25-jul-2017	6:57:00 PM	8:27:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
36	26-jul-2017	8:53:00 AM	10:23:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
37	26-jul-2017	11:00:00 AM	12:30:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
38	26-jul-2017	2:23:00 PM	3:53:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
39	26-jul-2017	4:00:00 PM	5:30:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
40	26-jul-2017	5:38:00 PM	7:08:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
41	26-jul-2017	7:12:00 PM	8:42:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
42	27-jul-2017	9:02:00 AM	10:32:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
43	27-jul-2017	10:41:00 AM	12:11:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
44	27-jul-2017	3:02:00 PM	4:32:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
45	27-jul-2017	4:39:00 PM	6:09:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
46	28-jul-2017	9:05:00 AM	10:35:00 AM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
47	28-jul-2017	10:42:00 AM	12:12:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
48	28-jul-2017	2:06:00 PM	3:36:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
49	28-jul-2017	5:41:00 PM	7:11:00 PM	1:30:00	190.237.149.52 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	179.7.139.175	50	0	0,00%	100,00%
50	9-ago-2017	10:01:00 AM	11:31:00 AM	1:30:00	190.235.51.28 / 192.168.1.24	Activo	190.233.83.100	Denegado/Anomalía	182.67.2.25	50	0	0,00%	100,00%
											PROMEDIO	0,00%	100,00%

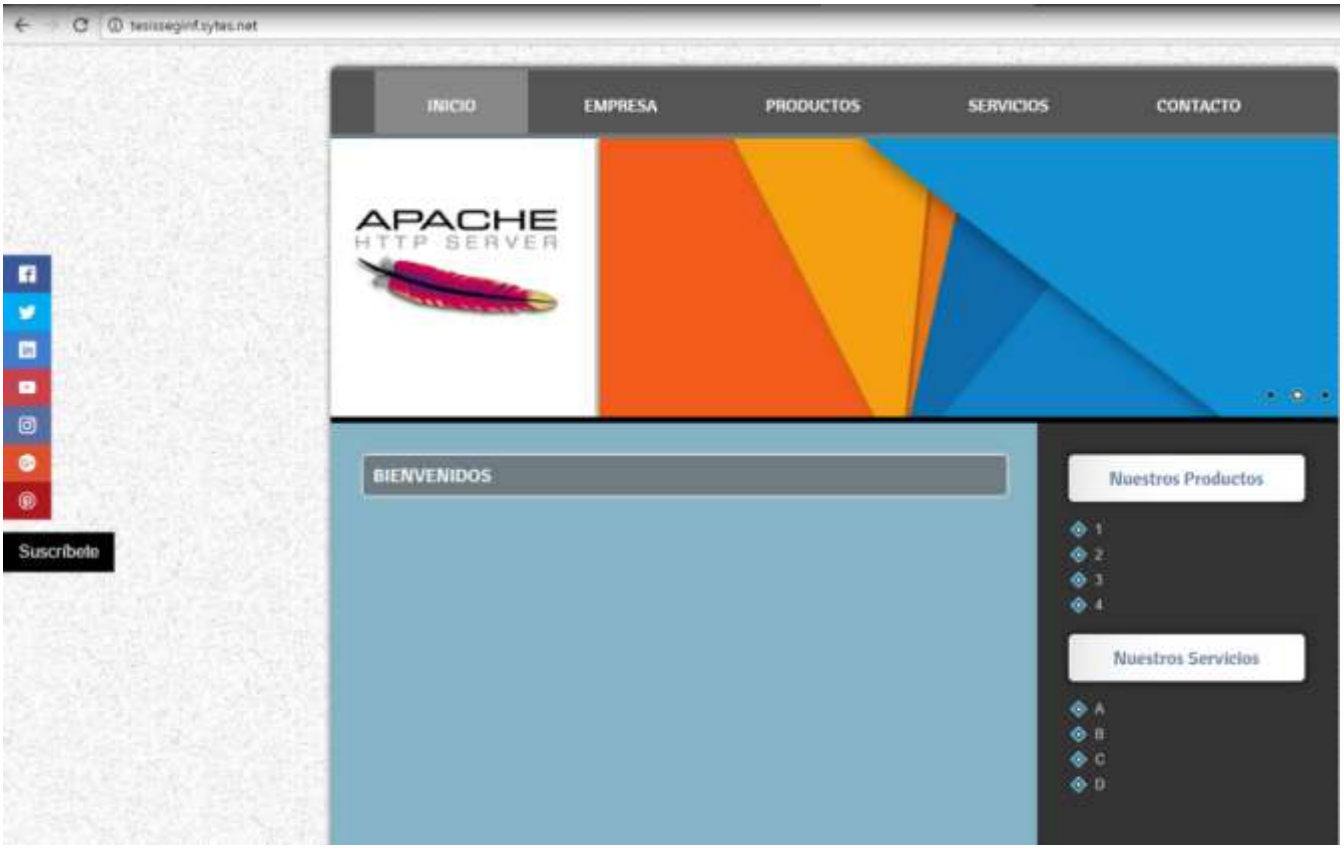
- **CONFIGURACIÓN DEL MÓDULO QOS, PARA LA PREVENCIÓN Y DETECCIÓN DE ATAQUES DDOS.**

```
 GNU nano 2.2.6                    Archivo: /etc/apache2/mods-available/qos.conf

<IfModule qos_module>
  # block clients violating some basic rules frequently (don't allows more than 20
  # violations within 5 minutes):
  QS_ClientEventBlockCount 20 300
  QS_SetEnvIfStatus       400             QS_Block
  QS_SetEnvIfStatus       401             QS_Block
  QS_SetEnvIfStatus       403             QS_Block
  QS_SetEnvIfStatus       404             QS_Block
  QS_SetEnvIfStatus       405             QS_Block
  QS_SetEnvIfStatus       406             QS_Block
  QS_SetEnvIfStatus       408             QS_Block
  QS_SetEnvIfStatus       411             QS_Block
  QS_SetEnvIfStatus       413             QS_Block
  QS_SetEnvIfStatus       414             QS_Block
  QS_SetEnvIfStatus       417             QS_Block
  QS_SetEnvIfStatus       500             QS_Block
  QS_SetEnvIfStatus       503             QS_Block
  QS_SetEnvIfStatus       505             QS_Block
  QS_SetEnvIfStatus       QS_SrvMinDataRate QS_Block
  QS_SetEnvIfStatus       NullConnection  QS_Block

  # allows privileged access to a single resource:
  SetEnvIf     Request_URI /server-status         QS_VipRequest=yes
  SetEnvIf     Request_URI /qos                   QS_VipRequest=yes

  # limits access to *.gif files to 100 concurrent requests:
  QS_LocRequestLimitMatch      "^.*\.gif$"            100

  # limits the connections for this virtual host:
  QS_SrvMaxConn                                  100

  # allows max 50 connections from a single ip address:
  QS_SrvMaxConnPerIP                              30

  # restricts max concurrent requests for any location which has no
  # individual rule:
  QS_LocRequestLimitDefault                          200

  # minimum request rate (bytes/sec at request reading):
  #QS_SrvRequestRate                              120

  # allows keep-alive support till the server reaches 600 connections:
  QS_SrvMaxConnClose                             600

^G Ver ayuda      ^O Guardar        ^R Leer Fich      ^Y RePág.         ^K Cortar Texto   ^C Pos actual
^X Salir          ^J Justificar     ^W Buscar         ^V Pág. Sig.      ^U PegarTxt       ^T Ortografía
```

- **DETECCIÓN DE LOS ATAQUES QOS, A TRAVÉS DE LA IP PÚBLICA, ADEMÁS CON DENEGACIÓN DE ACCESO.**

```
[Wed Aug 09 10:47:01.269859 2017] [:error] [pid 5408] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=31, c=190.233.83.100
[Wed Aug 09 10:47:01.270628 2017] [:error] [pid 5409] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=32, c=190.233.83.100
[Wed Aug 09 10:47:01.271125 2017] [:error] [pid 5410] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=33, c=190.233.83.100
[Wed Aug 09 10:47:01.271946 2017] [:error] [pid 5411] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=34, c=190.233.83.100
[Wed Aug 09 10:47:01.272567 2017] [:error] [pid 5412] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=35, c=190.233.83.100
[Wed Aug 09 10:47:01.273347 2017] [:error] [pid 5413] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=36, c=190.233.83.100
[Wed Aug 09 10:47:01.273788 2017] [:error] [pid 5414] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=37, c=190.233.83.100
[Wed Aug 09 10:47:01.274771 2017] [:error] [pid 5415] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=38, c=190.233.83.100
[Wed Aug 09 10:47:01.275156 2017] [:error] [pid 5416] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=39, c=190.233.83.100
[Wed Aug 09 10:47:01.276014 2017] [:error] [pid 5417] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=40, c=190.233.83.100
[Wed Aug 09 10:47:01.276694 2017] [:error] [pid 5418] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=41, c=190.233.83.100
[Wed Aug 09 10:47:02.278495 2017] [:error] [pid 5419] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=42, c=190.233.83.100
[Wed Aug 09 10:47:02.280058 2017] [:error] [pid 5420] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=43, c=190.233.83.100
[Wed Aug 09 10:47:02.281426 2017] [:error] [pid 5422] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=44, c=190.233.83.100
[Wed Aug 09 10:47:02.281912 2017] [:error] [pid 5423] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=45, c=190.233.83.100
[Wed Aug 09 10:47:02.283458 2017] [:error] [pid 5424] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=46, c=190.233.83.100
[Wed Aug 09 10:47:02.285162 2017] [:error] [pid 5425] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=47, c=190.233.83.100
[Wed Aug 09 10:47:02.285553 2017] [:error] [pid 5426] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=48, c=190.233.83.100
[Wed Aug 09 10:47:02.287108 2017] [:error] [pid 5427] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=49, c=190.233.83.100
[Wed Aug 09 10:47:02.288012 2017] [:error] [pid 5428] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=50, c=190.233.83.100
[Wed Aug 09 10:47:02.300214 2017] [:error] [pid 5447] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=70, message repeated 20 times,
c=190.233.83.100
[Wed Aug 09 10:47:03.300475 2017] [:error] [pid 5456] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=79, message repeated 20 times,
c=190.233.83.100
[Wed Aug 09 10:47:03.323920 2017] [:error] [pid 5476] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=30, concurrent connections=99, message repeated 20 times,
c=190.233.83.100
[Wed Aug 09 10:47:03.325316 2017] [:error] [pid 5478] mod_qos(030): access denied, QS_SrvMaxConn rule: max=100, concurrent connections=101, c=190.233.83.100
[Wed Aug 09 10:47:03.325822 2017] [:error] [pid 5479] mod_qos(030): access denied, QS_SrvMaxConn rule: max=100, concurrent connections=102, c=190.233.83.100
[Wed Aug 09 10:47:03.326759 2017] [:error] [pid 5480] mod_qos(030): access denied, QS_SrvMaxConn rule: max=100, concurrent connections=103, c=190.233.83.100
```

I. PÁGINA WEB PROPIA DESARROLLADA Y UTILIZADA PARA LOS ATAQUES DDOS.



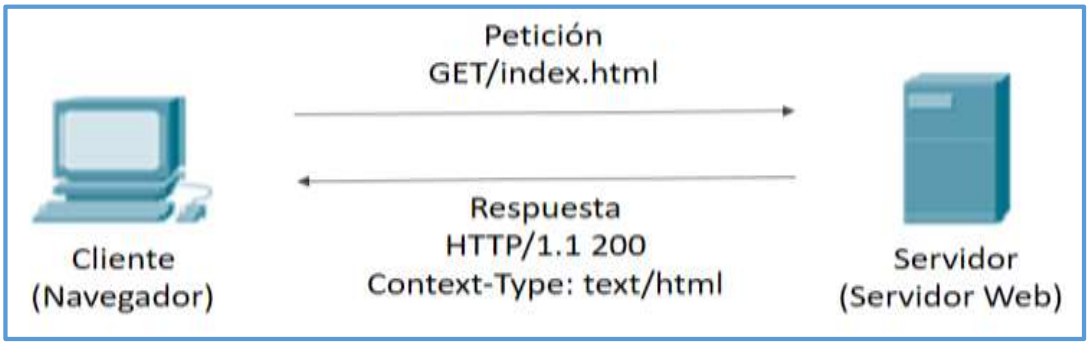
II. NUESTRO NOMBRE DE DOMINIO FUE ASIGNADO GRACIAS A UN SISTEMA DNS GRATUITO PARA OBTENER UN DOMINIO FIJO, ESTE SERVICIO ES CONOCIDO COMO NO-IP.

Fuente: Elaboración propia.

tesisseginf.sytes.net

Fuente: Elaboración propia.

III. EL FUNCIONAMIENTO ESQUEMÁTICO DEL PROTOCOL HTTP ES EL SIGUIENTE:



Fuente: Elaboración propia.

IV. EJEMPLO DE LA VERSION UTILIZADA EN LA CABECERA HTTP.

```
GET /index.html HTTP/1.1 HOST: www.tesisseginf.sytes.net
```

Fuente: Elaboración propia.