UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Esquema de seguridad contra ataques DoS y DDoS, Caso: Diario de Quintana Roo

TESIS
Para obtener el grado de
Ingeniero en Redes

PRESENTA
Rogelio Armando Tello Padilla

DIRECTOR DE TESIS
MSI. Laura Yésica Dávalos Castilla

ASESORES
MTI. Vladimir Veniamin Cabañas Victoria
Dr. Homero Toral Cruz
MTI. Melissa Blanqueto Estrada
Dr. Freddy I. Chan Puc

Chetumal Quintana Roo, México, diciembre de 2013

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Trabajo de Tesis elaborado bajo supervisión del Comité de asesoría

y aprobado como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo de Tesis

Directora: _____

MSI. Laura Yésica Dávalos Castilla

Asesor: _____

MTI. Vladimir Veniamin Cabañas Victoria

Asesor: _____

Dr. Homero Toral Cruz

Chetumal, Quintana Roo, México, Diciembre de 2013.

Dedicatoria

Por tu paciencia y comprensión sacrificaste tiempo que hubiéramos podido pasar juntos, permitiendo así que yo alcanzara una meta que hiciste tuya también. Cuando me sentí cansado me reanimaste, cuando desistí me fortaleciste; llegaste a ser un verdadero apoyo en todo aspecto necesario y eso es una verdadera muestra de amor. Te amo y por eso quiero dedicarte este trabajo Liliana León Cordero.

Agradecimientos

Te agradezco madre Dulce María Padilla Cárdenas, porque estuviste dispuesta a apoyarme por mucho tiempo a pesar de la difícil situación por la que atravesaste.

Gracias mami Dora Cárdenas González por soportarme por varios años en tu hogar y por todo lo que eso implicó para ti.

Gracias tía Guadalupe Padilla Cárdenas por estar pendiente de mí, cuando necesité de verdad no hubo nadie más que tú, cuando me faltó apoyo estuviste ahí.

A la MSI Laura Dávalos Castilla por el interés que demostró en mi crecimiento profesional le agradezco, la recordaré no solo como maestra, también como una buena amiga.

Gracias a los maestros que estuvieron siempre dispuestos a proporcionarme las herramientas que necesito para sobrevivir en la vida real.

Agradezco a la compañía Editorial del Sureste S.A. de C. V. por permitirme realizar los trabajos de esta tesis utilizando sus recursos de Hardware y software.

Resumen

El crecimiento exponencial de Internet trae consigo la necesidad de proteger cierta información que se comparte a través de ese medio, por ejemplo datos confidenciales de alguna empresa privada o información muy delicada sobre la vida personal o profesional de algún individuo. Sin mencionar sistemas críticos que se ejecutan en servidores remotos, donde los usuarios deben accesar para realizar ciertas transacciones, intercambiar, procesar y consultar datos.

El crecimiento de usuarios conectados es proporcionalmente directo al crecimiento de las medidas de seguridad en los nuevos procedimientos para compartir información. Si bien es cierto que las vulnerabilidades en las aplicaciones Web, generalmente se encuentran en la capa de aplicación del modelo OSI, pues son el resultado de escritura defectuosa del código; independientemente de los métodos de codificación que el programador utilice para proteger sus aplicaciones, el punto más crítico hoy en día son los servidores Web.

Actualmente es común escuchar de ataques dirigidos principalmente a los servidores Web, que hacen que el sitio no esté disponible por algún tiempo, este tipo de ataques se les denomina denegación de servicios y denegación de servicios distribuido (DoS y DDoS) “un ataque de denegación de servicio es cualquier acción, iniciada por una persona o cualquier otra causa, que incapacite al hardware, software, o ambos, de su *host* y que lleve a que no se pueda llegar a su sistema y después deniegue el servicio de legitimar (o incluso deslegitimar) usuarios. En un ataque DoS o DDoS, el objetivo del atacante es sencillo: sacar a su *host(s)* de la red”. (1). Para este caso específico, entenderemos como ataques de denegación de servicios al flujo masivo de peticiones al servidor Web a través del protocolo TCP/IP.

En este proyecto se pretenden aplicar medidas y políticas de seguridad para proteger de los ataques antes mencionados a la aplicación del sistema de noticias online del Diario de Quintana Roo con dominio http://www.dqr.com.mx. Dicha aplicación está implementada usando Joomla! “es un sistema de gestión de contenidos[CMS] galardonado que le permite crear y administrar fácilmente los

contenidos de un sitio web.” (2) Este CMS es de código abierto, lo que supone una ventaja pues aparte de su bajo costo es posible modificarlo para adaptarlo a nuestras necesidades. Aunque esto también supone un problema puesto que todas sus vulnerabilidades están abiertamente expuestas a cualquier atacante.

El servidor web que aloja al sistema de noticias online del Diario de Quintana Roo fue implementado en apache 2 es un servidor Web altamente configurable de diseño modular.

Aunque no existe un entorno completamente seguro, en este trabajo se pretende implementar medidas de seguridad utilizando herramientas que mitiguen los ataques más comúnmente utilizados hoy en día para dañar disponibilidad del sistema de noticias online del Diario de Quintana Roo.

Contenido

DEDICATORIA ..... **I**

AGRADECIMIENTOS ..... **II**

RESUMEN ..... **III**

INTRODUCCIÓN **3**

ANTECEDENTES **4**

DEFINICIÓN DEL PROBLEMA **4**

OBJETIVO GENERAL 6
OBJETIVOS ESPECÍFICOS 6
JUSTIFICACIÓN 6
ALCANCES Y RESTRICCIONES 7
METODOLOGÍA 8

MARCO TEÓRICO **9**

MARCO CONCEPTUAL 10
MARCO TEÓRICO 12
Sistema Operativo *12*
Servidor Apache *13*
Módulos de Apache *14*
Ataques DoS y DDoS *15*
Herramientas de ataque y monitoreo *16*
MARCO CONTEXTUAL 17
Antecedentes históricos *18*
¿Cómo son actualmente? *20*
Misión *21*
Visión *21*
Valores *21*
Objetivo general *22*

DESARROLLO **24**

IMPLEMENTACIÓN DE ATAQUES 25
IMPLEMENTACIÓN DE APACHE MOD_EVASIVE 32
IMPLEMENTACIÓN DE APACHE MOD_SECURITY 38

CONCLUSIONES **43**

ANEXO A **46**

ANEXO B **52**

BIBLIOGRAFÍA **54**

Figuras y Tablas

Figura 1 Ejecución de comando lsb_release –a en servidor web del Diario de Quintana Roo 12
Figura 2Ejecución de comando apache2 –version en servidor web del Diario de Quintana Roo 13
Figura 3 Arquitectura interna de Apache, “sacado de La Biblia del Servidor Apache, de Kabir, Mohammed J.” 14
Figura 4 Sistema de noticias online del Diario de Quintana Roo 25
Figura 5 Prueba de ataque controlado 27
Figura 6 Ejecución de la herramienta netstat 27
Figura 7 Resultado de netstat 29
Figura 8 Inhabilitación del sistema de noticias online del Diario de Quintana Roo 30
Figura 9 Iniciando del servidor web apache 30
Figura 10 Estado de Nagios 31
Figura 11 Instalación mod-evasive 32
Figura 12 Creación de directorio 33
Figura 13 Asignación de derechos 33
Figura 14 Archivo de configuración mod evasive.conf 33
Figura 15 contenido del archivo de configuración mod_evasive.conf 34
Figura 16 Activación del módulo 35
Figura 17 Ejecución mod evasive 35
Figura 18 Resultado de la ejecución del script test.pl 36
Figura 19 Ejecución del monitorieo del ataque 36
Figura 20 Evasión del ataque DoS, monitoreo netstat 37
Figura 21 Ejecución del comando aptitude para realizar la instalación de la librería lib-apache-mod-security 38
Figura 22 Instalación mode security 39
Figura 23 Ejecución del comando mkdir para crear el directorio “modsecurity” 39
Figura 24 Ejecución del comando mkdir para crear el directorio “modsecurity_data” 40
Figura 25 Ejecución del comando ln para que los logs del apache mod security aparezcan en el registro principal del logs del apache 40
Figura 26 Listado de reglas que bloquean ataques del tipo DoS o DdoS 41
Figura 27 Reinicio de apache 41
Figura 28 Resultado del bloqueo 42
Figura 29 Script perl para probar el apache mod_evasive 53

Tabla 1 Archivo mod_evasive20.so 47

Introducción

Antecedentes

El departamento en seguridad en cómputo de la Universidad Autónoma de México/UNAM-CERT junto con la colaboración de Andrés Romero Mier y Terán y Mauricio Andrade, el 10 de marzo de 2009 publicó la tutoría llamada “Aspectos Básicos de la Seguridad en Aplicaciones Web” donde encontramos una breve descripción de los problemas esenciales de seguridad en las aplicaciones Web y algunos consejos sobre cómo solucionarlos. Las sugerencias descritas en esta tutoría aportan al presente documento la guía necesaria para aplicar algunas técnicas de mitigación de ataques más frecuentes.

Definición del problema

Con el surgimiento de nuevas tecnologías y la implementación de las mismas en las grandes empresas, se solucionan problemas y satisfacen necesidades; sin embargo estas traen consigo la aparición de nuevas vulnerabilidades en los sistemas, mismos que pueden ser aprovechados por cualquiera con intenciones de hacer daño o conseguir información confidencial que pueda proporcionarle algún provecho. Dada la proposición anterior, entendemos que la seguridad es subjetiva, es decir, que las medidas de seguridad (hardware, software o políticas de seguridad) para una empresa pudieran o no ser aplicables a otra compañía con las mismas características o el mismo giro, esto significa que no puede haber un estándar de seguridad que pudiera funcionar para todos los casos.

Debido a lo anterior es necesario hacer un análisis de los equipos críticos del Diario de Quintana Roo para protegerlo de posibles daños al hardware o al software. En el caso específico del sistema de noticias del Diario de Quintana Roo, se reviste de marcada importancia económica y social, debido a las siguientes razones:

- El sistema de noticias online del Diario de Quintana Roo provee a sus anunciantes un espacio publicitario donde se exponen sus productos o servicios, y a los clientes potenciales que visitan la página se les permite mantenerse informados sobre el acontecer diario de la vida Quintanarroense, junto con la posibilidad de obtener los datos de los anunciantes para consumir algún producto o servicio presentado en la aplicación web. Para que un anunciante pueda tener acceso a este servicio debe pagar una tarifa dependiendo del tipo de servicio publicitario que le interese. La exposición de los anuncios en el sistema de noticias trae consigo la posibilidad de que el anunciante capte más clientes, que al final de cuentas redunda en mayores ingresos.

- El sistema de noticias online del Diario de Quintana Roo tiene el compromiso social de mantener informada a la población sobre el acontecer diario de la vida quintanarroense, y cada día miles de usuarios utilizan internet para acceder a las noticias más importantes del estado publicadas en dicha aplicación. El que algún ataque malicioso por parte de un hacker dañara la integridad de la información o la disponibilidad del sitio, haría que se esté faltando a este compromiso y pondría en duda el prestigio y reputación de la empresa.

Con lo anterior se subraya la trascendencia de mantener cierto grado de seguridad para el servidor web, por eso surge la siguiente pregunta:

¿Qué medidas de seguridad se pueden implementar en el servidor Web del sistema de Noticias Online del Diario de Quintana Roo para mitigar ataques del tipo DoS o DDoS, y qué políticas pueden aplicarse en caso de ser objetivo de algún ataque?

La tutoría “Aspectos Básicos de la Seguridad en Aplicaciones Web” propone algunas recomendaciones generales para evitar problemas de seguridad. En este trabajo implementaremos algunas de las sugerencias dadas en este estudio y se comprobará la utilidad de las mismas.

Para proveer de cierto nivel de seguridad al Sistema de Noticias del Diario de Quintana Roo las acciones son las siguientes.

Mitigar los ataques DoS dirigidos al servidor apache, que consisten básicamente en lanzar peticiones legítimas al servidor web pero de forma masiva, tratando de colapsar el mismo. Al utilizar el módulo apache mod_evasive se consigue redirigir el tráfico de dichas peticiones a un error y el apache mod_security sirve de WAF (Web application Firewall, o Firewall para la aplicación web), mitigando no sólo ataques DDoS sino también otros tantos, aplicando reglas de filtrado.

Objetivo general

Implementar medidas de seguridad en el Servidor Web del Sistema de Noticias del Diario de quintana Roo para mitigar ataques del tipo DoS o DDoS, y aplicar políticas en caso de ser objeto de dichos ataques.

Objetivos específicos

Implementar los módulos de apache mod_evasive y mod security para mitigar ataques DoS y DDoS y redirigir el tráfico del puerto 80 del protocolo TCP/IP al puerto 403 error de conexión.

Crear y Aplicar políticas de monitoreo de las conexiones al servidor apache con el comando netstat.

Justificación

La tecnología aplicada de las herramientas que se van a implementar puede proveer de integridad, disponibilidad y confidencialidad a la aplicación del sistema de noticias online del Diario de Quintana Roo.

Se tiene la desagradable experiencia que en ocasiones anteriores la aplicación Web del Diario de Quintana Roo ha colapsado por varias horas debido a ataques DoS, también una intrusión por parte de un hacker tuvo como consecuencia la eliminación de las noticias del sitio.

Esto muestra que el sistema de Noticias del Diario de Quintana Roo es muy vulnerable a los tipos de ataques antes mencionados y para evitar que los usuarios del sitio vayan a la competencia para satisfacer sus necesidades de información cuando la página no esté disponible hay que garantizar la funcionalidad.

Dicho sea de paso que con la caída del sitio Web el Diario de Quintana Roo experimentaría la pérdida de usuarios, prestigio, clientes etc. Con la consecuente pérdida económica.

Alcances y restricciones

Para lograr los objetivos antes mencionados se divide el trabajo por etapas en las que se realizarán los análisis, instalaciones y/o configuraciones correspondientes para cada caso. Dichas etapas son las siguientes:

Análisis. De acuerdo a la experiencia obtenida debido a ataques anteriores, se identificaron los tipos de ataques más frecuentes y de igual modo se detectaron algunas vulnerabilidades, lo anterior permite definir las medidas de protección, una vez hecho esto también se obtienen las bases para establecer políticas de monitoreo de los sistemas críticos.

Implementación. Una vez detectadas las vulnerabilidades, se procede a implementar el software y su configuración correspondiente para este caso específico, así como las políticas de seguridad que permitirán mitigar algún posible ataque.

Pruebas. Mediante el uso de algunas herramientas se simulan algunos ataques controlados para probar la resistencia del servidor. Para determinar un mejor nivel de seguridad apropiado para el servidor, se deben realizar pruebas continuamente hasta lograr un resultado satisfactorio.

Monitoreo. Se debe utilizar el software instalado para monitoreo del sistema, cabe señalar que el administrador de servidores ya ha utilizado y probado el uso de herramientas como netstat y Nagios.

Soporte continuo. Como todo software, políticas y herramientas de control, se necesita un mantenimiento continuo de las tecnologías aplicadas para su buen funcionamiento, durante el tiempo en el que según las condiciones del servidor, todo lo aportado en este trabajo siga siendo la mejor solución para los problemas detectados.

Todas las implementaciones y configuraciones de software para mitigación de ataques Dos se realizan sobre el servidor web del Diario de Quintana Roo, a menos que se indique lo contrario y debido a que el sistema de noticias alojado en dicho servidor en el que se harán las pruebas debe verse afectado lo menos posible, todo experimento se efectúa en un ambiente controlado, en una hora en la que no haya tantos usuarios del sitio.

Por eso dichas pruebas se realizaron al terminar con la edición del día, aproximadamente a las dos de la mañana.

Metodología

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

1. Lograr exponer la vulnerabilidad del servidor web, comprometiéndolo ante situaciones de ataques del tipo DoS o DDoS reales y monitorizados.
2. Implementar las herramientas evasivas de ataque.
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 los módulos realicen su trabajo, documentar los errores, localizar las causas, repararlas y generar acciones de prevención.

Se considera un éxito, el que las herramientas efectúan las tareas de evasión de ataques del tipo DoS o DDoS.

Marco Teórico

Para fijar con claridad y exactitud el significado de las acciones para proteger el sistema de noticias del Diario de Quintana Roo http://www.dqr.com.mx es necesario enunciar las propiedades de las ideas expresadas por el autor de este trabajo, posteriormente delimitar las características del conjunto de procedimientos, estrategias y herramientas a utilizar para este caso específico; con el fin de diferenciarlas de las demás existentes.

Marco conceptual

Detectar. Mediante herramientas informáticas o de deducción empírica, localizar o descubrir alguna anomalía, virus o persona que esté oculta, es decir, que no se pueda percibir su presencia fácilmente, o con los medios tradicionales.

Analizar. Se refiere a la separación de alguna situación, cosa o intenciones para estudiar los elementos que lo componen, con el fin de determinar patrones de comportamiento o tomar medidas de control o protección. Para este estudio generalmente, se utilizará este término para referirse al comportamiento del tráfico en la red, cuando y donde una computadora o dispositivo está enviando mensajes, de qué tipo son y si es posible detectar algún contenido malicioso para suprimir la comunicación de esa computadora con el resto de la red.

Implementar. Poner en marcha alguna acción, sistema o política para cumplir con alguna función específica ya sea de protección o seguridad informática o cualquier otra función útil para la red.

Políticas. Consiste en establecer métodos y técnicas organizacionales para detectar y solucionar fallas y debilidades en la seguridad de sistemas o equipos críticos, lo cual implica renovar y actualizar herramientas de software o hardware cuando estas son vulnerables, de igual modo para que las políticas de seguridad sean verdaderamente útiles, deben estar sujetas a los cambios que se adapten a las necesidades de la organización y a las nuevas tecnologías que se desarrollan o implementan para suplir dichas necesidades.

Ataque. Para efectos de esta investigación, es el intento de cualquier intruso de penetrar o burlar la seguridad de la red para tener acceso a información confidencial o desactivar e incluso dañar algún equipo de hardware o un software importante, de gestión o publicación de la información de la empresa.

Ataque DDOS (Distributed Denial of Service). Es un ataque que tiene como objetivo colapsar un sistema de red o servidores para evitar que los usuarios legítimos tengan acceso a él, esto se hace a través de un flujo masivo de peticiones por medio del protocolo TCP/IP a través de varios puntos de conexión.

Apache. Servidor web para protocolo HTTP multiplataforma, que incorpora la noción de sitio virtual, también el servidor es altamente configurable de diseño modular, lo cual significa que sus funciones pueden ser ampliadas escribiendo un módulo en los lenguajes C o perl y añadiéndolos al sistema.

Módulos de apache. Apache ofrece directivas las cuales se distribuyen en módulos, dichos módulos añaden funcionalidad al servidor web y son configurables.

Hash. Una tabla hash o mapa hash es una estructura de datos que asocia llaves o claves con valores. La operación principal que soporta de manera eficiente es la búsqueda: permite el acceso a los elementos (direcciones IP, por ejemplo) almacenados a partir de una clave generada.

Scripts. Conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos.

Logs. Es el registro de actividad del sistema operativo, en este caso, son usados para asentar cualquier ataque del tipo DoS o DDoS contra el servidor apache.

Seguridad. Es cualquier acción encaminada a proteger información valiosa, puede ser confidencial, privilegiada o pública, según la empresa lo considere. Dicha información comprende, entre otras cosas, software, bases de datos o archivos así como cualquier cosa que la empresa valore.

Monitoreo del servidor. Implica el uso de un sistema previamente instalado por el administrador para constatar el buen funcionamiento de la red y de los sistemas instalados, facilitar la detección de alguna anomalía y descubrir alguna amenaza exterior por parte de algún intruso, o buscar algún problema de sobrecarga o falla de los equipos críticos en la red.

Marco teórico

Sistema Operativo

La plataforma en la que está instalado el servidor web es Linux, la distribución es Ubuntu server 10.04.02 LTS, información que se puede obtener ejecutando el siguiente comando:

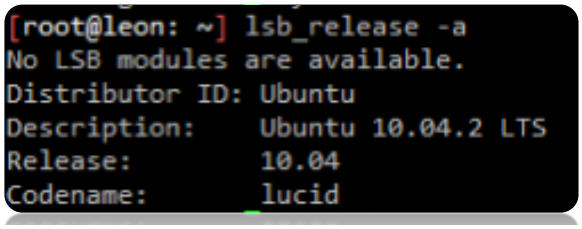


Figura 1 Ejecución de comando lsb_release –a en servidor web del Diario de Quintana Roo

Es importante decir que dicho servidor no tiene instalada ninguna interfaz gráfica de escritorio. Al igual que la mayoría de las distribuciones de Linux, Ubuntu es gratuito y libre, es decir, puede obtenerse sin costo alguno y el soporte con actualizaciones tampoco genera algún precio. Puede descargarse la última versión de este sistema operativo en la página oficial de Ubuntu http://www.ubuntu.com/.

Ubuntu proporciona un entorno robusto y funcional, adecuado para la implementación de servidores y clientes que soportan los protocolos y mecanismos esenciales para proporcionar distintos servicios de red, entre los que se incluyen:

- TCP (*Transmission Control Protocol*, Protocolo de Control de Transmisión)
- IP (*Internet Protocol*, Protocolo de Internet)
- SSH (*Secure Shell,* Interprete de comandos seguro)
- Apache (Servidor web)

- HTTP (*Hypertext transfer Protocol*, Protocolo de Transferencia de Hipertexto)
- HTML (*HyperText Markup Language,* Lenguaje de Marcado de Hipertexto)
- PHP (*PHP Hypertext Pre-processor* inicialmente *Personal Home Page Tools*)
- MysQL (*My Structured Query Language*, es decir, Mi Lenguaje de Consulta Estructurado)

Que para efectos de la presente investigación son los que más usaremos.

Servidor Apache

Apache es un servidor web multiplataforma, que permite indexación de directorios, uso de sobrenombres con las carpetas, informes configurables sobre errores http, ejecución de programas CGI y que además admite la última versión del protocolo http/1.1. (3)

La versión instalada en el servidor web del *Diario de Quintana Roo* es apache 2.2.14. Información que se puede obtener ejecutando el siguiente comando:

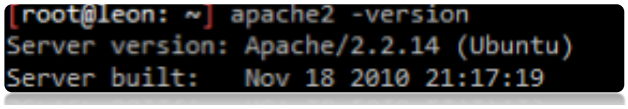


Figura 2Ejecución de comando apache2 –version en servidor web del Diario de Quintana Roo

Este servidor web, se compone de un núcleo, creado desde el código de Apache, y una serie de módulos adicionales que son los que van a definir la manera de trabajar del mismo. Muchos de estos módulos ya vienen compilados en la instalación predeterminada, pudiendo añadir más funcionalidad a nuestro servidor, o bien eliminando aquellos que no se van a utilizar. (3)

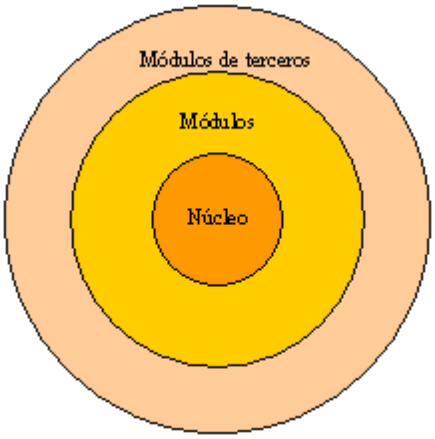


Figura 3 Arquitectura interna de Apache, "sacado de La Biblia del Servidor Apache, de Kabir, Mohammed J."

En el caso de este trabajo se pretende agregar funcionalidad al servidor, protegiéndolo de peticiones maliciosas que pudieran colapsarlo, evitando así que los usuarios legítimos del sistema de noticias online tengan acceso a la información correspondía al día en que suceda un ataque DoS o DDoS.

Módulos de Apache

Es muy sencillo ampliar las capacidades del servidor Web Apache. Cualquiera que posea una experiencia decente en la programación de C o Perl puede escribir un módulo para realizar una función determinada. Esto significa que hay una gran cantidad de módulos Apache para su utilización. (4)

mod_evasive es un módulo para Apache que proporciona una acción evasiva en el caso ataques DoS o DDoS HTTP o de fuerza bruta. También está diseñado para ser una herramienta de detección y gestión de la red, y puede ser fácilmente configurado para comunicarse con ipchains, firewalls, routers, etcétera. mod_evasive también rinde informes de abusos a través de servicios de correo electrónico y syslog. (5)

mod_security es un firewall de aplicaciones web (WAF). Con más de 70% de los ataques ya realizados sobre el nivel de aplicación Web, las organizaciones necesitan toda la ayuda que puede obtener en la toma de sus sistemas de

seguridad. WAF se implementan para establecer un nivel mayor de seguridad externa para detectar y / o prevenir los ataques antes de que lleguen a las aplicaciones web. ModSecurity proporciona protección contra una serie de ataques contra aplicaciones web y permite el seguimiento del tráfico HTTP y análisis en tiempo real con pocos o ningún cambio a la infraestructura existente (6).

Como vemos el mod_evasive servirá para tener protección específica contra ataques DoS o DDoS, mientras que el mod_security servirá de firewall de aplicaciones Web evitando incluso otro tipo de ataques dirigidos al sistema de noticias online del Diario de Quintana Roo.

Ataques DoS y DDoS

A nivel básico un ataque de Denegación de Servicios (DoS) es cualquier acción iniciada por alguna persona o por cualquier otra causa, que incapacite al hardware, software o ambos, de su host y que lleve a que no se pueda llegar a su sistema y después deniegue el servicio de legitimar (o incluso deslegitimar) usuarios. En un ataque DoS, el objetivo del atacante es sencillo: sacar su host(s) de la Red. Excepto cuando los equipos de seguridad comprueban hosts consentidos, los ataques DoS son maliciosos y además ilegales. (1)

Los DDoS (*Distributed Denial of Service*) son ataques distribuidos de denegación de servicio, es decir, se trata de igual manera de colapsar servidores pero a través de distintos puntos de conexión no solamente de uno.

Este tipo de ataques hoy en día son comúnmente realizados para colapsar aplicaciones web y evitar que estas puedan ofrecer sus servicios a clientes o usuarios legítimos. Esto se realiza Mediante un software malicioso que a través del protocolo TCP/IP envía peticiones legitimas por el puerto 80 al servidor web.

Este tipo de ataques se han extendido por todo el mundo, debido a la facilidad con la que se llevan a cabo. Sirva como botón de muestra los ataques realizados en diciembre de 2010 a las empresas que le dieron la espalda a la organización WikiLeaks. “El grupo 'Anonymous' se atribuyó los ciberataques del miércoles (8 de

diciembre de 2010) contra las compañías estadunidenses de tarjetas de crédito MasterCard y Visa, así como de otras empresas que bloquearon los medios de financiación de WikiLeaks o de su fundador, el australiano Julian Assange… El vocero que es un ingeniero de software, de 22 años de edad, precisó que cada vez más gente se está bajando la herramienta 'Botnet' que permite llevar a cabo los llamados ataques de Denegación de Servicio Distribuidos (DDos) (7).” Dicho sea de paso, esto se convirtió en noticia internacional y sirvió para que mucha gente conociera y hasta se familiarizara con las herramientas como ‘Bootnet’ que se usaron para efectuar los ataques antes mencionados. Por eso se hace cada vez más necesario prepararse para afrontar algún ataque de denegación de servicios.

Sin embargo, desde antes que el ‘caso WikiLeaks’ sucediera, durante los meses de junio y julio del año 2010 el sistema de noticias online del *Diario de Quintana Roo* fue “objeto de un ataque DoS que sobrecargó el servidor apache e hizo que este colapsara, en el primer caso por un lapso de más de dos horas. No se pudo hacer nada para mitigar el ataque que hasta concluir, nos permitió volver a activar los servicios.” (8)

Herramientas de ataque y monitoreo

Para lograr mitigar los ataques antes mencionados al servidor web del *Diario de Quintana Roo,* se requiere de ciertas herramientas de software que permitirán acometer ciertos ataques controlados y otras para realizar mediciones exactas para obtener la cantidad de peticiones que soporta el servidor actualmente sin estar protegido. Algunas de las herramientas que se enlistan a continuación han sido previamente instaladas por el administrador de servidores del departamento de Cómputo y Telemática del Diario de Quintana Roo.

Netstat. (estadísticas de red) es una herramienta de línea de comandos que muestra las conexiones de red (tanto entrantes como salientes), tablas de enrutamiento, y una serie de estadísticas de la interfaz de red. Está disponible en Linux, Unix, Windows y sistemas operativos basados en NT. (9). Se utilizará netstat para el monitoreo del tráfico generado por los ataques realizados al servidor web.

Podremos ver la(s) dirección(es) ip origen o “atacante(es)” y el destino o “victima” y como es que antes de realizar las configuraciones de los módulos de apache, el ataque DDoS surte el efecto deseado por el “atacante”.

Nagios es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas (10). Esta herramienta permitirá monitorear el servidor web mostrando un informe detallado sobre su disponibilidad.

Http Attack. Software que realiza la función de generar tráfico TCP/IP a través del puerto 80. Mediante el uso de esta aplicación se realizarán ataques al servidor web del *Diario de Quintana Roo*, primero para ver lo que sucede sin disponer de protección alguna contra ataques DoS ó DDoS, finalmente se realizarán otras pruebas pero con la protección implementada.

Todo lo anterior servirá para la realización de las pruebas que permitirán, en primero lugar poner en evidencia la vulnerabilidad que posee el servidor, lo cual justificará las medidas que se deben tomar con tal de proveer de mayor seguridad al mismo. En segundo lugar, las mismas herramientas verificarán el correcto funcionamiento de los módulos de apache.

Marco Contextual

La Compañía Editorial del Sureste S.A. de C.V. se ubica en Av. Calzada Tampico No. 615, Esquina Ignacio Comonfort, Chetumal, Quintana Roo, México. En sus Instalaciones se ostenta el nombre de Diario de Quintana Roo, designación con el que a la empresa se le identifica con mayor facilidad. Fundada hace ya más de 25

años, tiempo en el que se ha consolidado como una de las más confiables fuentes de noticias en el estado.

Antecedentes históricos

Cómo nace Diario de Quintana Roo

Diario de Quintana Roo. “Integrado a la vida quintanarroense”, salió a la luz pública el 04 de noviembre de 1986, como el primer periódico de Quintana Roo, a iniciativa de un cúmulo de empresarios locales que arriesgaron su capital con el firme propósito de hacer un periódico local. Sin embargo ya existían franquicias de periódicos peninsulares y de otros lugares, que se mandaron a colocar en el estado, antes y después de la creación de Diario de Quintana Roo, siendo éste el primero de origen netamente quintanarroense.

La edición inicial fue de cuatro secciones de ocho páginas cada una con la portada y contraportada a color y todos los interiores en blanco y negro. En formato tradicional de ocho columnas, con un logotipo muy llamativo y representativo del nacimiento de un proyecto con muchas ilusiones. El proyecto se gestó desde meses atrás y las pruebas se efectuaron desde tres meses antes de la primera edición formal.

La parte informativa la proveían las agencias informativas Excelsior, UPI, Fransc Pees, y Reuter, vía télex, y un cuerpo informativo de tan sólo ocho reporteros comprometidos y entusiastas, dirigidos atinadamente por el reconocido periodista José Concepción “pimpo” Pereyra Lizárraga (q. d. e. p) primer Director Editorial.

La aparición de DQR causó furor en la entidad a pesar de la baja creencia de la sociedad, las páginas ilustradas con fotografías y caricaturas, escritas con noticias y opiniones locales, nacionales e internacionales, deportes, policiacas, sociales y económicas, no eran muy comunes entre la vida de los quintanarroenses. La creencia era sólo de lo que provenía de periódicos publicados en el DF, Mérida, Tabasco y Campeche.

La plantilla laboral con que inició actividades esta empresa fue de 25 personas entre reporteros, editores, redactores, correctores, diagramadores, fotógrafos, talleres de composición, fotomecánica, transporte, prensistas, repartidores y administrativos. De los cuales algunos iniciaron labores desde tres meses antes de salir a la luz pública en la etapa de pruebas y capacitación.

La vida de esta empresa, no podría pasar por alto la gran labor de “X-Hazil” la rotativa V15 de la prestigiosa marca Harris, provista por la empresa Maqui Van representante de la marca en México en ese entonces.

El primer ejemplar salió a la luz con una edición inicial de 7,000 ejemplares circulando en todo el estado y cuya impresión culminó alrededor de las diez de la mañana del día siguiente.

Los empresarios visionarios que apostaron a esta gran aventura son:

- Mario Rendón Monforte
- Roberto Borge Martín
- Abraham Farah Wejebe
- Diego Enrique Rojas Zapata
- Jorge Vargas de Regil (+)
- John N. Baroudi Estéfano
- Luis Felipe Buenfil Durán
- Eusebio Moguel Medrano (+)
- Antonio Marrufo Villanueva (+)

Y el líder del proyecto arquitectónico: Sergio A. Vázquez V.

¿Cómo son actualmente?

El difícil arranque se superó, a través de los años, consejeros de la administración de DQ, directores, editores, reporteros, impresores, publicistas, trabajadores de talleres y de oficinas administrativas, más los voceadores y anunciantes, toman conciencia de la gran responsabilidad para mantener bien informada a la población, y ahora, con un tiraje de 15,000 ejemplares DQR circula en todo el estado día a día con gran potencial en la preferencia de los lectores. Además, con cobertura en ruta en el estado hermano de Yucatán.

Y así, en 23 años se ha visto crecer a Diario de Quintana Roo, con nuevas creaciones de modernidad como la tecnología de punta, Internet y la recepción de cables que envían las agencias de noticias convenidas, que facilitan la obra diaria periodística comandada por el Licenciado Luis Antonio Contreras Castillo Presidente del Consejo de Administración y un grupo de profesionales en la materia, junto con el Director Editorial, Elder Vega Martínez, editores, redactores, publicistas, reporteros, esquemadores, fotógrafos, correctores, técnicos en sistemas de computación y un buen equipo de producción al mando del experimentado técnico en Artes Gráficas, Joel René Flores Blanquet, que hacen que diariamente salga a la luz pública Diario de Quintana Roo.

Actualmente la empresa tiene sucursales en toda la geografía estatal; Cancún en conjunto con Isla Mujeres y Kantunilkin; Cozumel; Playa del Carmen en conjunto con Puerto Morelos y Tulúm; Felipe Carrillo Puerto; José María Morelos; la ciudad de Mérida y las oficinas matrices en nuestra capital Chetumal.

La plantilla laboral está conformada por 210 trabajadores distribuidos en todas nuestras sucursales; una flotilla de equipo de reparto de 30 vehículos; y operando en el área de producción dos rotativas, la experimentada “X-hazil” Harris V-15 y la de reciente adquisición una Harris V-25.

A más de dos décadas, DQR forma gran parte en el seguimiento social y político que da parte, paso a paso, de los hechos más relevantes de la actualidad. Las primeras planas a todo color con el emisor de las noticias en las 64 páginas, en sus

ocho secciones, trasmiten a la opinión pública la información generada en la entidad y el país con el agregado visual de las imágenes fotográficas en blanco y negro y a todo color.

Lo cierto es que hoy Diario de Quintana Roo es un componente fundamental de la vida quintanarroense e inseparable de los sistemas políticos democráticos. El periodismo en DQR crea y causa opinión, por sus necesidades de lectura y tradición de la prensa escrita, con un estilo editorial único en la región, con la redacción que ha nutrido numerosos reporteros, redactores y escritores, los cuales forman parte de sus páginas y se destacan en sus columnas. Además DQR ha creado prestigiosos y serios comentarios en la vida social y política, por lo que ha causado y creado opinión día a día, y eso hace que se nutra más Diario de Quintana Roo.

Misión

Somos un periódico comprometido con los quintanarroenses, con el fin de mantenerlos informados de manera veraz y oportuna sobre el acontecer diario en la península, mediante un periodismo profesional, objetivo y de calidad para nuestros lectores.

Visión

Transformarnos en la empresa líder dentro del ramo de la información impresa, por el éxito y aceptación de nuestros clientes, destacándonos principalmente por emplear tecnología de vanguardia en la producción de nuestros ejemplares, contando además con un equipo de periodistas comprometidos con la sociedad en cuanto a informar de manera veraz y oportuna los acontecimiento que se dan día a día en el estado, el país y el mundo.

Valores

Los valores organizacionales son los que construyen la identidad de la empresa y forman la médula de la cultura corporativa. En el Diario de Quintana Roo, integrado a la vida quintanarroense; se viven los siguientes valores:

- **Compromiso:**

Reconocemos a la sociedad, nuestros clientes, proveedores y compañeros como los beneficiarios de nuestro trabajo, considerando la importancia de su participación en la determinación de nuestro rumbo. Por lo que nos comprometemos a poner al máximo nuestras capacidades para sacar adelante todo aquello que se nos ha confiado; lo hacemos de corazón yendo más allá de la firma de un documento, o un contrato. Cuando nos comprometemos es porque conocemos las condiciones que estamos aceptando y las obligaciones que éstas conllevan.

- **Verdad:**

Nos significa decir la verdad, y no sólo una vez, sino una y otra vez, de tal forma que sea una actitud permanente. La veracidad aporta algo claro y firme a todo el hombre, a su ser y a su actuación.

- **Objetividad:**

Exige de nosotros ver los problemas y las situaciones con un enfoque que equilibre adecuadamente emoción y razonamiento, porque nos permite dar su justo peso a los acontecimientos y obrar de una forma coherente.

- **Respeto:**

Reconocemos la autonomía y dignidad de cada persona aceptando complacidos el derecho a ser diferente, la regla: “tratar a los demás como nos gustaría ser tratados”.

- **Cooperación:**

El todo es más que la suma de las partes, por lo que trabajamos en equipo, respetando las diferencias, complementando esfuerzos y construyendo con las aportaciones de los demás.

Objetivo general

Crear y causar una opinión de nuestros lectores por medio del periodismo manejado a través de nuestra marca propia Diario de Quintana Roo, satisfaciendo con ello sus necesidades de lectura y tradición de prensa escrita, por medio de un estilo

editorial único en la región, con el fin de seguir creando prestigiosos y serios comentarios de la vida social y política.

Desarrollo

Implementación de ataques

Como ya se ha explicado anteriormente, el sistema de noticias online del *Diario de Quintana Roo*, se implementó usando las herramientas CMS joomla, que a su vez está desarrollada con PHP, java, xml, html y css como lenguajes de programación, MySQL como gestor de bases de datos y se ejecutan a través del servidor apache.

La apariencia del sistema de noticias online del *Diario de Quintana Roo* actualmente y en condiciones normales, es la siguiente:

Figura 4 Sistema de noticias online del Diario de Quintana Roo

Antes de realizar las implementaciones de los módulos de apache para la mitigación de ataques DoS y DDoS se realizaron pruebas que demostraron la vulnerabilidad del sitio. Dichos ensayos se realizaron en un ambiente controlado, es decir, con un miembro del departamento de cómputo y telemática del *Diario de Quintana Roo* observando el proceso, monitorizando el tráfico hacia al servidor web con la herramienta netstat esto nos permitió constatar la vulnerabilidad del apache. Un 'atacante' externo efectuó el envío masivo de peticiones por el puerto 80 del protocolo TCP/IP con la herramienta Http Attack. A continuación se describe paso a paso este proceso.

Configuración de la herramienta de ataque. Para el buen funcionamiento de Http Atack, tenemos que proporcionarle cierta información:

URL: se refiere a la dirección o nombre de dominio del sitio web que es el objetivo del ataque.

Proxy: Si el atacante se encuentra en una red administrada que implementa un servidor proxy, se debe especificar la dirección IP del proxy para que las peticiones se hagan a través de él.

Connections: El número total de conexiones que se va a solicitar al servidor web objetivo.

Connection rate: La tasa de conexiones que se generan por segundo, si la cantidad se establece en 1000 o más, las conexiones se generan lo más rápido posible.

Timeout(s): tiempo de espera, en segundos, entre cada escritura de paquetes. Pueden ser fracciones de segundo.

User-Agent: son los parámetros enviados en los encabezados de los paquetes http.

*Attack-Especific Parameter*s: Al estar deshabilitada esta opción por defecto, el método por el que se envían las peticiones es POST, el cual expide datos para que sean procesados por el servidor. En caso contrario, el método de petición es GET que se utiliza en la descarga de archivos.

En la siguiente imagen vemos los datos que fueron usados para la realización de la prueba de ataque controlado. Se observa que La URL del objetivo está definida como http://dqr.com.mx/index.php. Como el ataque se realizó desde una conexión Cable Más de hogar, donde no se usa ningún servidor proxy, no fue necesario colocar nada en ese campo, del parámetro de conexiones se configuró a 4000 y todo lo demás se dejó con los valores por defecto.

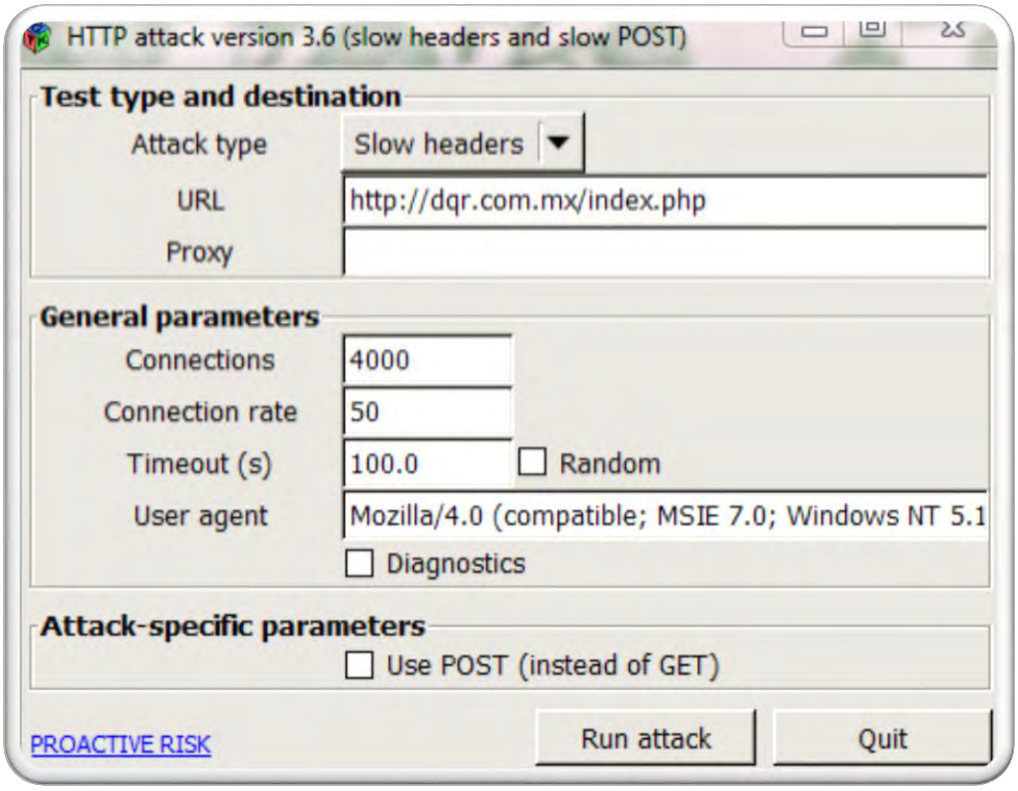


Figura 5 Prueba de ataque controlado

Esta prueba se realizó el día 07 de abril de 2011 a las 12:34 am. Durante el ataque, se ejecutó la herramienta Netstat en el servidor web para monitorear el tráfico generado por el 'atacante'.

La herramienta se ejecutó con los parámetros que se muestran en la siguiente imagen y que se explican a continuación:

Figura 6 Ejecución de la herramienta netstat

-a: Despliega todo lo solicitado en un listado.

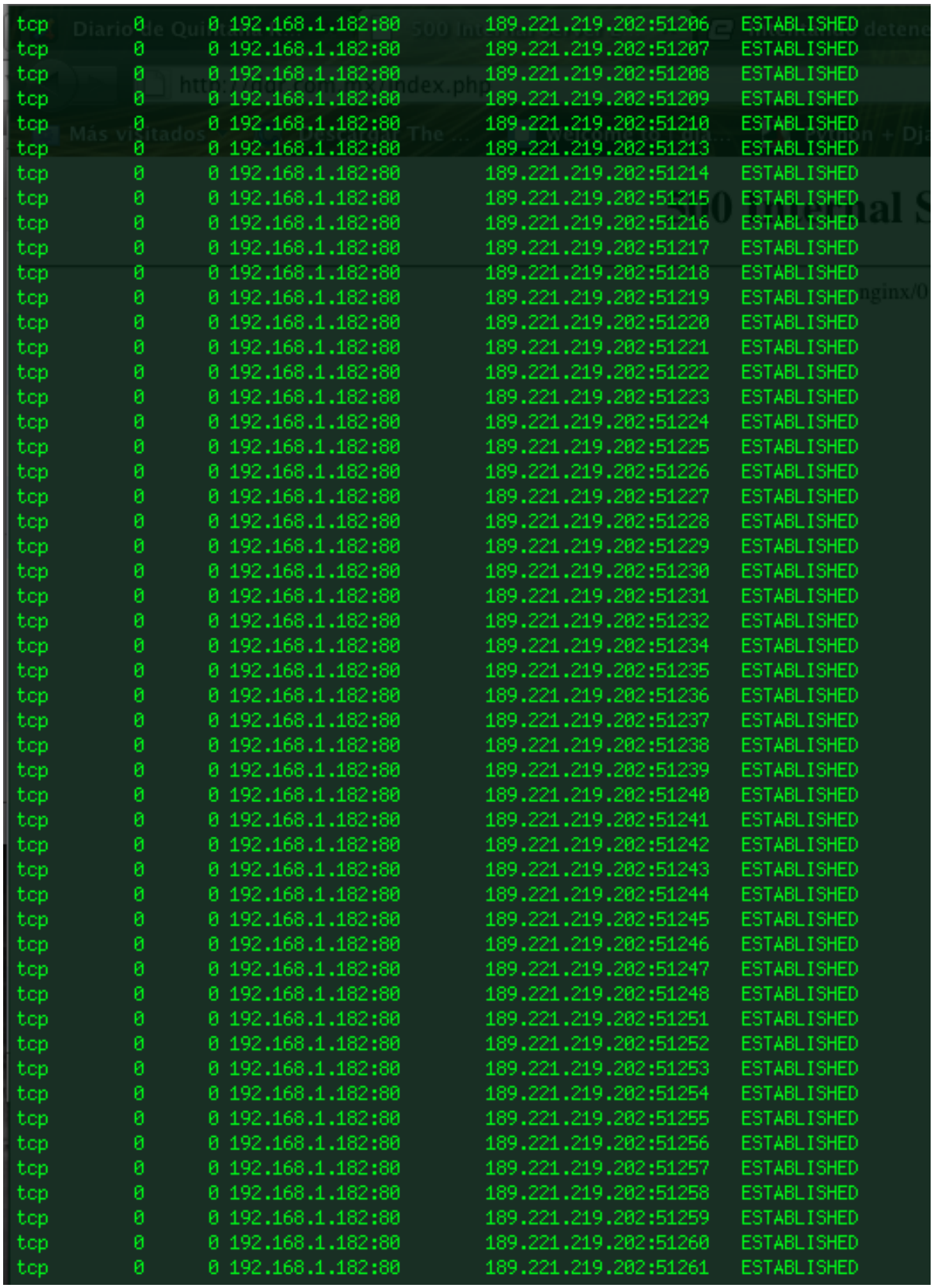
-n: Los datos se muestran en formato numérico.

grep: funciona como un filtro, pues servirá para mostrar únicamente el resultado solicitado en el siguiente parámetro.

80: combinado con grep, este parámetro sirve para mostrar únicamente el tráfico hacia el servidor web a través del puerto 80.

Sort: ordena el resultado de la búsqueda.

Durante el ataque el tráfico pudo observarse la dirección ip del servidor local 192.168.1.182 y también la del 'atacante' 189.221.219.202, se observan que todas las solicitudes fueron atendidas por el servidor. Figura 7.



tcp	0	0	192.168.1.182:80	189.221.219.202:51206	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51207	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51208	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51209	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51210	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51213	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51214	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51215	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51216	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51217	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51218	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51219	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51220	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51221	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51222	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51223	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51224	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51225	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51226	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51227	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51228	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51229	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51230	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51231	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51232	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51234	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51235	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51236	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51237	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51238	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51239	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51240	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51241	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51242	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51243	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51244	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51245	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51246	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51247	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51248	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51251	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51252	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51253	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51254	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51255	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51256	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51257	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51258	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51259	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51260	ESTABLISHED
tcp	0	0	192.168.1.182:80	189.221.219.202:51261	ESTABLISHED

Figura 7 Resultado de netstat

.

Como es lógico, todas las solicitudes hechas al servidor fueron atendidas lo que ocasionó que este colapsara incluso antes de terminar con el envío de las 4000 peticiones configuradas en la herramienta Http Attack y cómo podemos ver en la siguiente imagen el servidor apache fue derribado al cabo de aproximadamente minuto y medio después de haber empezado el ataque, con la consecuente inhabilitación del sistema de noticias online del *Diario de Quintana Roo.*

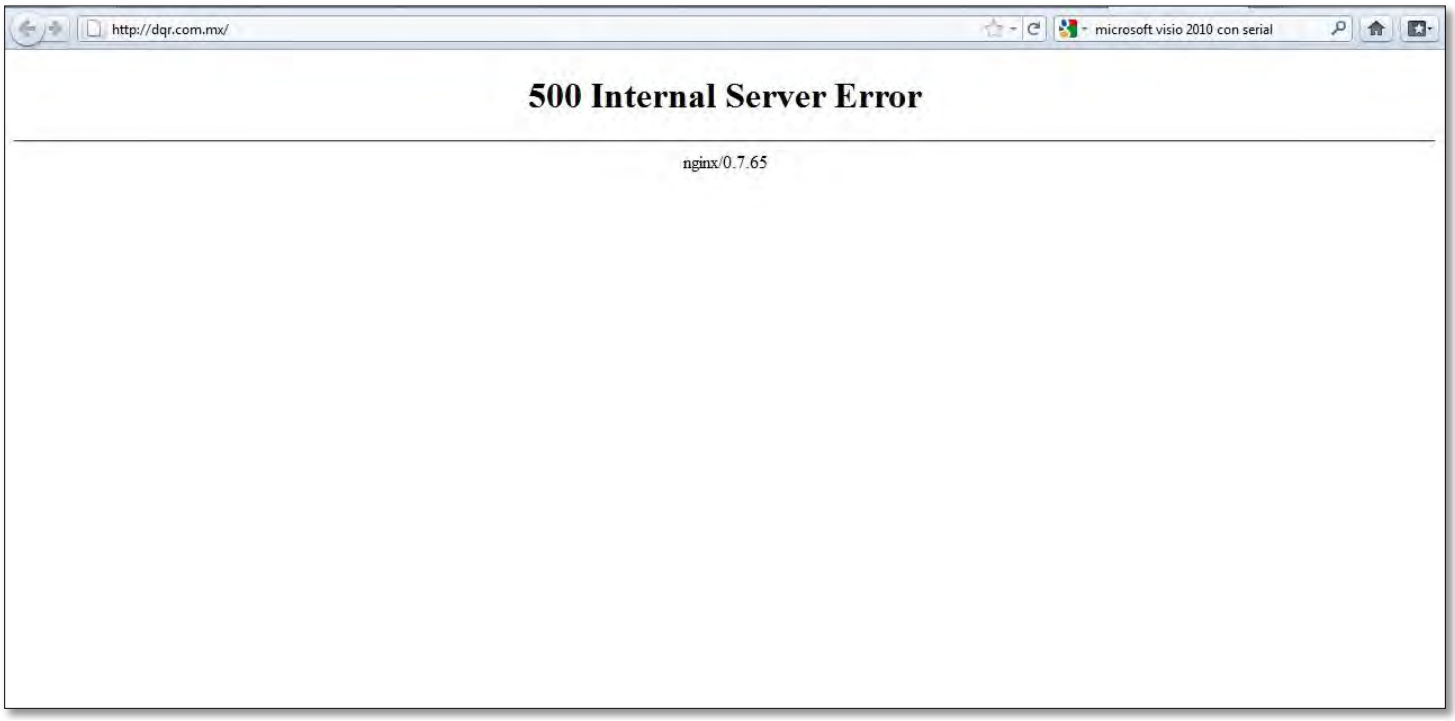


Figura 8 Inhabilitación del sistema de noticias online del Diario de Quintana Roo

Después de concluido el ataque y verificar la caída del servidor, se procedió a levantar el servicio de apache de la siguiente manera:

```
[root@leon: ~] /etc/init.d/apache2 start
 * Starting web server apache2
[root@leon: ~]                                    [ OK ]
```

Figura 9 Iniciando del servidor web apache

El sistema de monitorización de redes Nagios detectó la caída del apache, aunque por la misma razón que el sistema de noticias, no se pudo consultar

inmediatamente, sí mostró un reporte posterior que indicó que el servidor web había caído. La consulta se realizó después de levantar nuevamente el apache.

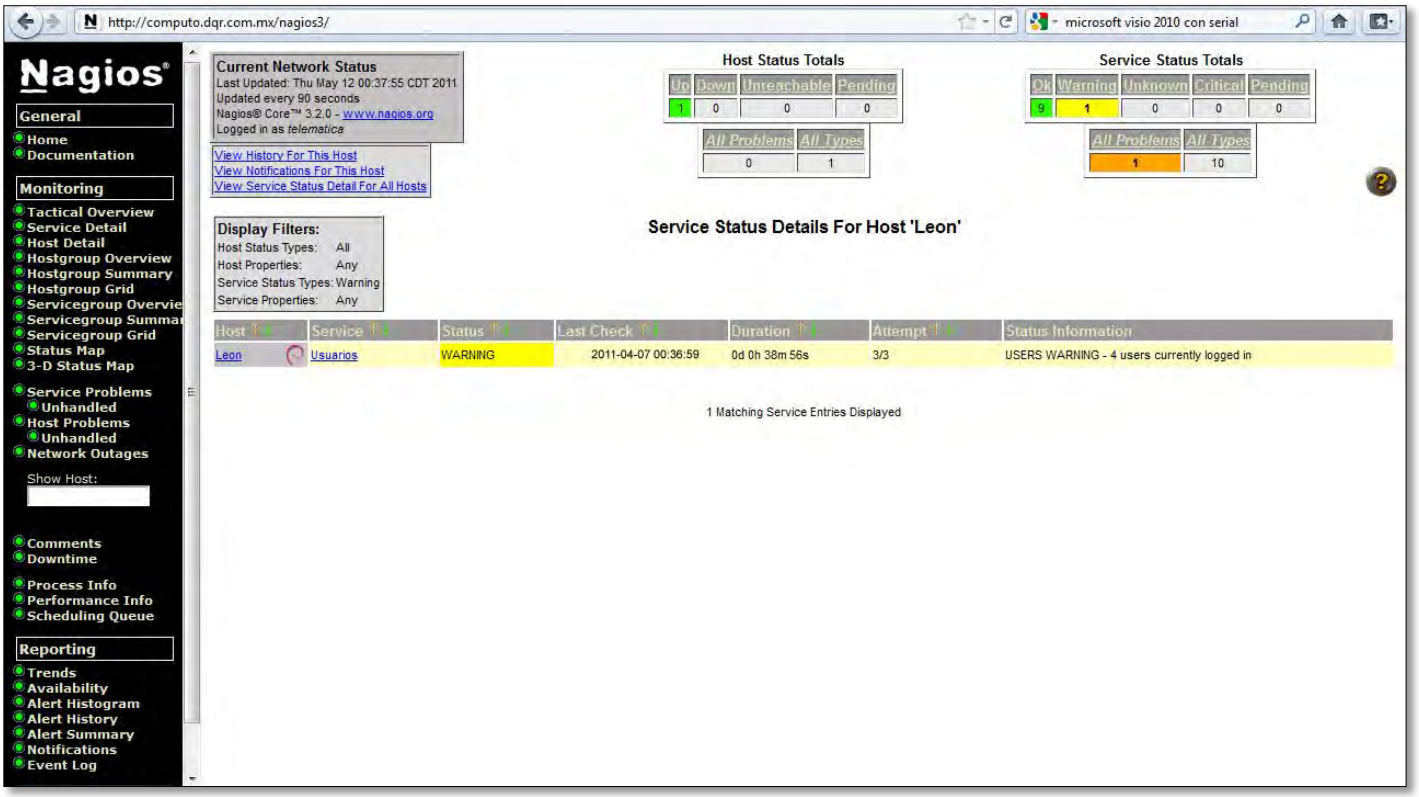


Figura 10 Estado de Nagios

El status que indica el Nagios es WARNING o alerta, pues revela que el servicio proporcionado a los usuarios de la aplicación web ha tenido un problema el día 07 de abril del 2011 a las 00;36:59. Con esto queda revelada la vulnerabilidad del servidor web ante los ataques del tipo DoS y DDoS, lo cual justifica la implementación de los módulos de apache que mitigan las conexiones maliciosas al servidor web.

Implementación de apache mod_evasive

mod_evasive Es un módulo que integra estrategias evasivas en el servidor apache, es decir, en caso de un ataque DoS o DDos proporciona una acción evasiva al redirigir el tráfico de peticiones ilegítimas del puerto 80 del protocolo TCP/IP hacia un error 403 (prohibido).

La detección se realiza mediante la creación de una tabla hash interna dinámica de direcciones IP y URIs, negando cualquier dirección IP que realice cualquiera de las siguientes acciones:

- Hacer más de dos peticiones a la misma página por segundo.
- Hacer más de 50 solicitudes simultáneas en el mismo child process por segundo.
- Seguir realizando solicitudes después de haber sido registrado en una lista de bloqueo.

Debido al diseño de peticiones per-child, las peticiones legitimas no se ven comprometidas (incluso las que vienen de servidores Proxy o de direccionamiento NAT), sólo bloquea los ataques de secuencias de comandos (5).

Instalación.

Para realizar la instalación, recurrimos al método apt-get, donde se extrae e instala el apache mod_evasive desde la dirección oficial garantizada del paquete.

```
[root@leon:~]apt-get install libapache2-mod-evasive
```

Figura 11 Instalación mod-evasive

Con esto, se han instalado los siguientes archivos:

Mod-evasive.load. En el directorio mods-aviable y mods-enable del apache, que sirve para cargar el módulo al momento de ejecutar el servidor.
Mod_evasive20.so. En el directorio 'usr/lib/apache2/modules/mod_evasive20.so' que es donde se encuentra el código fuente del módulo apache mod_evasive. (Ver anexo No 1)

Seguidamente debemos crear el directorio donde se almacenarán los logs del mod_evasive.

```
[root@leon:~] mkdir /var/log/apache2/mod_evasive
```

Figura 12 Creación de directorio

Seguidamente, asignamos los derechos de administrar el fichero de los logs al usuario del sistema que corresponde al servidor apache.

```
[root@leon:~] chown www-data:www-data /var/log/apache2/mod_evasive
```

Figura 13 Asignación de derechos

Se crea el archivo de configuración del apache mod_evasive.conf, en el directorio /etc/apache2/conf.d/

```
[root@leon:~] vi /etc/apache2/conf.d/01_modevasive.conf
```

Figura 14 Archivo de configuración mod evasive.conf

Y se le agregó los siguientes parámetros:

```
<ifmodule mod_evasive20.c>
 DOSHashTableSize 3097
 DOSPageCount 2
 DOSSiteCount 50
 DOSPageInterval 1
 DOSSiteInterval 1
 DOSBlockingPeriod 10
 DOSLogDir /var/log/apache2/mod_evasive
 DOSEmailNotify computo@dqr.com.mx
 DOSWhitelist 127.0.0.1
</ifmodule>
```

Figura 15 contenido del archivo de configuración mod_evasive.conf

DOSHashTableSize. Establece el número de nodos a almacenar para cada proceso de peticiones de la tabla hash. Cuanto más grande sea el tamaño de la tabla de Hash, más memoria requerirá, pero el rastreo de direcciones IP será más rápido. Para el caso del servidor del *Diario de Quintana Roo*, no es necesario aumentar el valor por defecto, pues el número de peticiones no es tan grande.

DOSPageCount. Indica el valor del umbral para el número de peticiones de una misma página (o URI) dentro del intervalo definido en DOSPageInterval. Cuando el valor del parámetro es excedido, la IP del cliente se añade a la lista de bloqueos. En este caso pondremos que el valor máximo de solicitudes es de 2.

DOSSiteCount. Cuenta cuántas peticiones de cualquier tipo puede hacer un cliente dentro del intervalo definido en DOSSiteInterval. Si se excede dicho valor, el cliente queda añadido a la lista de bloqueos. El número máximo de peticiones es de 50.

DOSPageInterval. El intervalo, en segundos, para el máximo de peticiones de páginas.

DOSSiteInterval. El intervalo, en segundos, para el umbral de petición de objetos de cualquier tipo.

DOSBlockingPeriod. Establece el tiempo, en segundos, que un atacante queda bloqueado una vez que ha sido añadido a la lista de bloqueos. Como ya se indicó unas líneas atrás, todo cliente bloqueado recibirá una respuesta del tipo 403 (Forbidden) a cualquier petición que realice durante este periodo. Si el atacante lo sigue intentando, este contador se reseteará automáticamente, haciendo que siga más tiempo bloqueada la IP.

DOSLogDir. Establece una ruta para el directorio donde se almacenarán los Logs.

DOSEmailNotify. Dirección de correo electrónico que recibirá información sobre los ataques.

DosWhitelist. Podemos especificar una IP o rango que será excluido del rastreo por mod_evasive. Para este caso solamente excluiremos al mismo servidor apache.

Seguidamente se realiza la activación del módulo

```
[root@leon:~] a2enmod mod-evasive
```

Figura 16 Activación del módulo

Comprobación del apache mod_evasive

Entre las utilidades del software, se descargó un script Perl llamado test.pl que se localiza en el directorio /usr/share/doc/libapache2-mod-evasive/examples/. El cual, y como su nombre lo indica, permite la comprobación del funcionamiento del apache mod_evasive.

Para ejecutarlo se escribe el siguiente comando:

```
[root@leon:/usr/share/doc/libapache2-mod-evasive/examples/#] perl test.pl
```

Figura 17 Ejecución mod evasive

El resultado fue el siguiente:

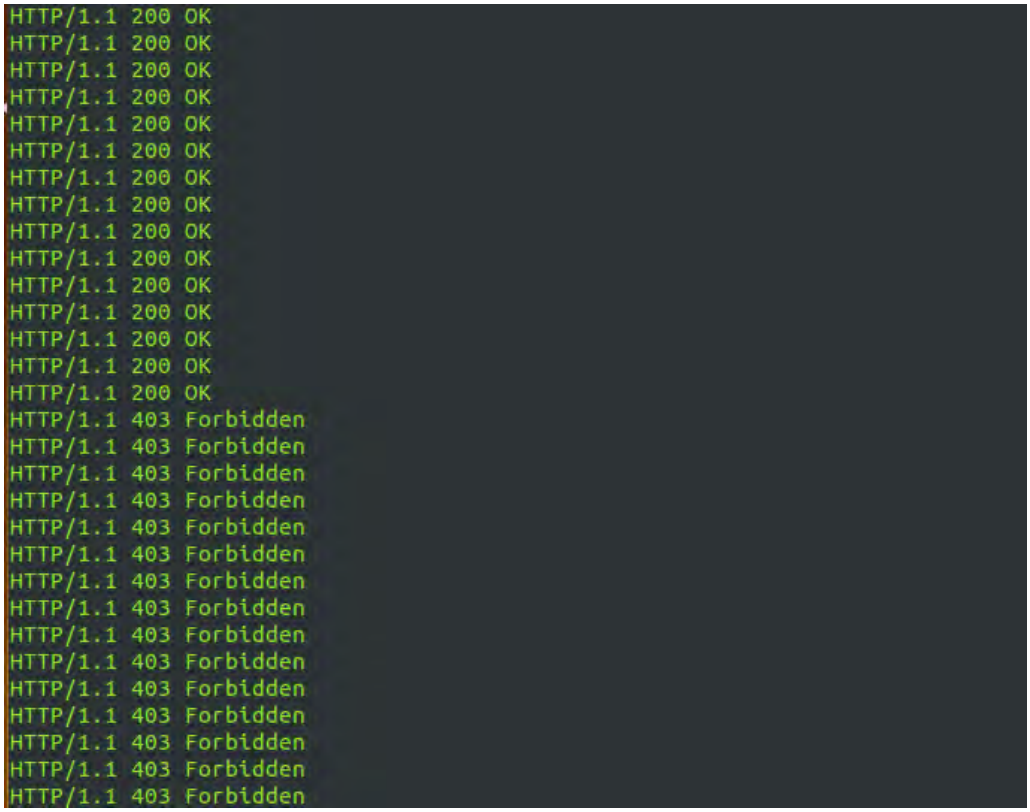


Figura 18 Resultado de la ejecución del script test.pl

De esto se deduce que las configuraciones del apache mod_evasive son correctas y están listas para soportar un ataque real.

Para realizar la comprobación del funcionamiento del apache mod_evasive se realizó una prueba el día 08 de mayo de 2011 a las 12:43 am. Durante el ataque, se ejecutó la herramienta Netstat en el servidor web para monitorear el tráfico generado por el 'atacante'.

Para monitorear el ataque utlizaremos el mismo comando netstat usado y explicado anteriormente

Figura 19 Ejecución del monitorieo del ataque

El resultado del ataque es el siguiente:

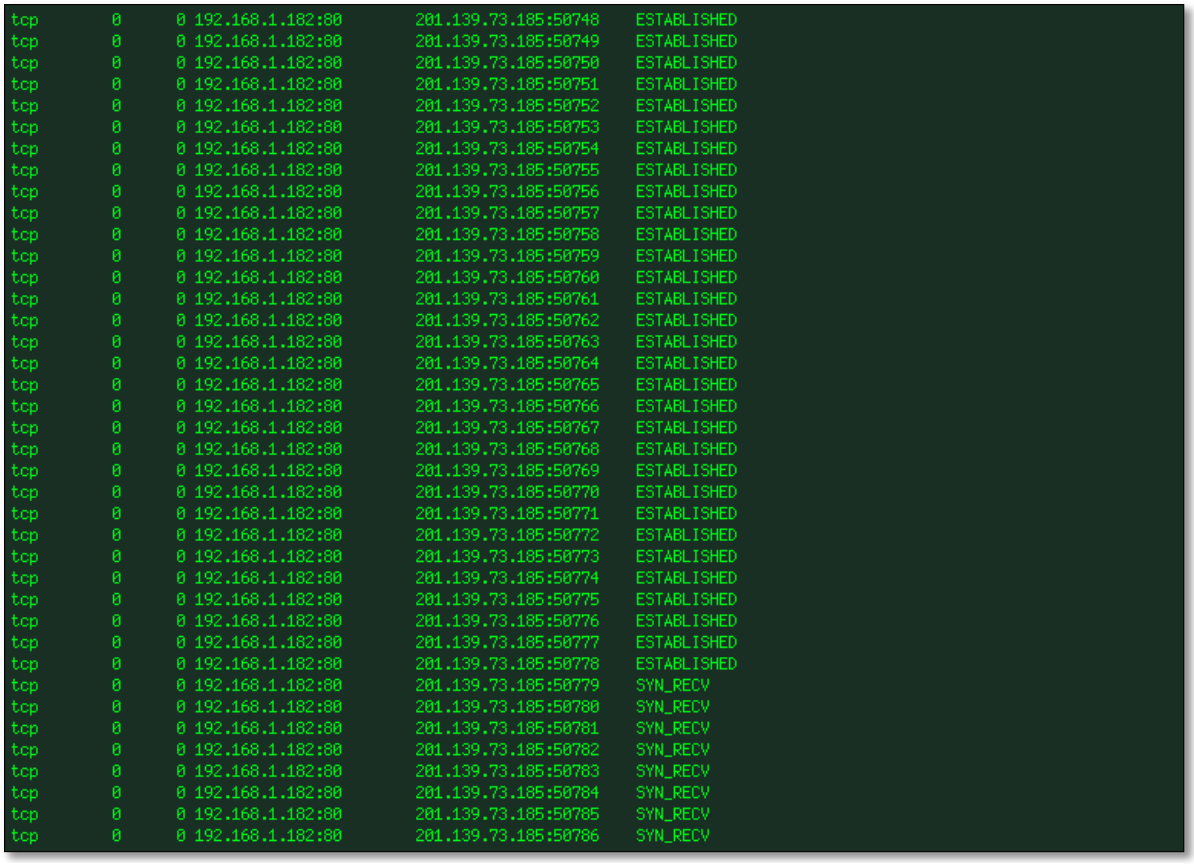


Figura 20 Evasión del ataque DoS, monitoreo netstat

Como vemos en esta imagen el ataque fue evadido, pues las solicitudes del atacante fueron retrasadas después de las 50 peticiones simultaneas y finalmente la dirección IP fue bloqueada

El ataque duró aproximadamente dos minutos culminando el día 08 de mayo de 2011 a las 12:46 a.m.

Con esto, se comprueba el correcto funcionamiento del apache mod_evasive ante un ataque real, monitoreado, del tipo DdoS

Implementación de apache mod_security

El apache mod security es un WAF (Web Application Firewall) que “podría definirse como un dispositivo, plugin del servidor o un conjunto de reglas que filtran y analizan el tráfico web (entre tu servidor web y tu red externa), es decir, los datos que recibimos por parte del usuario y la respuesta que nuestro servidor web arrojará al usuario. Prácticamente se encuentra de intermediario entre [la] aplicación y el servidor web que la tiene alojada” (11). Siendo un software del tipo firewall especializado en aplicaciones web, sirve como una herramienta para administrar las conexiones al servidor a través del puerto 80 del protocolo TCP/IP, proporcionando así cierta protección de una serie de ataques contra dichas aplicaciones web.

Para este caso específico se implementará este software y se aplicarán sus reglas de filtrado, para proteger al servidor web del Diario de Quintana Roo contra ataques DoS o DdoS.

El primer paso de la implementación es la instalación del modulo Apache mod_security ejecutando el comando que se muestra a continuación:

Figura 21 Ejecución del comando aptitude para realizar la instalación de la librería lib-apache-mod-security

Tras la ejecución, del comando anterior, mientras se realiza la descarga, el instalador pide autorización para realizar la descarga de 1027KB de archivos comprimidos, que al descomprimirse ocuparán 2966KB de espacio en disco, para continuar hay que introducir “Y”.

```
root@leon: # aptitude install libapache-mod-security
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Initializing package states... Hecho
Writing extended state information... Hecho
The following NEW packages will be installed:
  libapache-mod-security mod-security-common{a}
0 packages upgraded, 2 newly installed, 0 to remove and 58 not upgraded.
Need to get 1027kB of archives. After unpacking 2966kB will be used.
Do you want to continue? [Y/n/?] Y
Writing extended state information... Hecho
Get:1 http://mx.archive.ubuntu.com/ubuntu/ lucid/universe mod-security-common 2.5.11-1 [914kB]
Get:2 http://mx.archive.ubuntu.com/ubuntu/ lucid/universe libapache-mod-security 2.5.11-1 [114kB]
Fetched 1027kB in 18s (54.2kB/s)
Seleccionando el paquete mod-security-common previamente no seleccionado.
(Leyendo la base de datos ...  00%
67342 ficheros y directorios instalados actualmente.)
Desempaquetando mod-security-common (de .../mod-security-common_2.5.11-1_all.deb) ...
Seleccionando el paquete libapache-mod-security previamente no seleccionado.
Desempaquetando libapache-mod-security (de .../libapache-mod-security_2.5.11-1_i386.deb) ...
Configurando mod-security-common (2.5.11-1) ...
Configurando libapache-mod-security (2.5.11-1) ...
 * Reloading web server config apache2
   ...done.

Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Reading extended state information
Initializing package states... Hecho
Writing extended state information... Hecho
```

Figura 22 Instalación mode security

Hay que aclarar que se instaló la herramienta que permite la creación e interpretación de las reglas de filtrado, lo que sigue es realizar un script que contenga las reglas para su posterior ejecución.

Para esto se crea un directorio en /etc/apache2/conf.d con el nombre de modsecurity de la siguiente manera:

```
root@leon:/# mkdir /etc/apache2/conf.d/modsecurity_
```

Figura 23 Ejecución del comando mkdir para crear el directorio "modsecurity"

Con esto tenemos todo preparado para realizar un archivo de configuración donde indicaremos las reglas de filtrado que evitan que un ataque DoS o DDoS logre su objetivo mediante rechazar las peticiones hechas al servidor.

También se debe crear y enlazar un directorio donde se guardarán los logs del apache modsecurity.

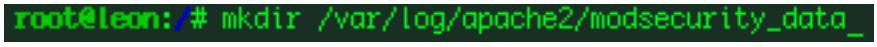


Figura 24 Ejecución del comando mkdir para crear el directorio "modsecurity_data"

A continuación enlazamos el directorio creado en el paso anterior con el directorio en el que ModSecurity crea los logs por defecto.

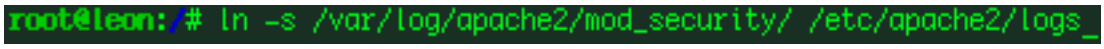


Figura 25 Ejecución del comando ln para que los logs del apache mod security aparezcan en el registro principal del logs del apache

Hecho lo anterior se procede a la creación de las reglas de filtrado del archivo que nos permitirá evadir los ataques DoS o DdoS.

Las directivas que se deben usar para la realización del script son las siguientes:

SecRuleEngine: Directiva que controla si se procesan las reglas de filtrado. Se debe poner en On si la versión del mod instalada no lo hiciera ya por defecto.

SecAuditLogType: configura el tipo de mecanismo de la auditoria de logs que va a ser usado.

SecAuditLog: Define la ruta principal del archivo de registro de los logs.

SecDataDir: Define el directorio en los que se guardarán datos de los logs.

SecRule: es la directiva principal del apache Mod_Security. Sirve para analizar datos y realizar acciones basadas en los resultados (12).

Luego de haber realizado la instalación, ahora toca indicarle a Apache que lea las reglas y las ejecute. Para esto entramos al archivo /etc/apache2/apache2.conf con el editor de textos y agregamos la siguiente línea:

```
Include /etc/apache2/modsecurity/*.conf
```

Con lo cual, se le indica al Apache que debe leer todos los archivos .conf del directorio /etc/apache2/conf.d/modsecurity que es donde se deben guardar las reglas de filtrado. Ahora bien, se agrega el un Script que realiza el bloqueo automático de las direcciones ip atacantes. A continuación se muestra el contenido del archivo donde se ejecuta el listado de reglas que bloquean ataques del tipo DoS o DdoS que han sido guardadas en el directorio /etc/apache2/conf.d/modsecurity/ con el nombre de “mod_security_Dos.conf”

```
SecRuleEngine On
SecAuditEngine RelevantOnly
SecAuditLogType Serial
SecAuditLog logs/mod_security.log

# Directorio donde mod_security almacenará los logs
SecDataDir /var/log/apache2/modsecurity_data

# ignora las peticiones provenientes de localhost otra IP
SecRule REMOTE_ADDR "^127\.0\.0\.1$" "phase:1,nolog,allow"

# para todas las peticiones a urls por IP/seg
# (incremento de las solicitudes var por cada uno, expira en 1 segundo)
SecRule REQUEST_BASENAME
"!(\.avi$|\.bmp$|\.css$|\.doc$|\.flv$|\.gif$|\
---------------------------
\.htm$|\.html$|\.ico$|\.jpg$|\.js$|\.mp3$|\
---------------------------
\.mpeg$|\.pdf$|\.png$|\.pps$|\.ppt$|\.swf$|\
---------------------------\.txt$|\.wmv$|\.xls$|\.xml$|\.zip$)"\
---------------------------
"phase:1,nolog,pass,initcol:ip=%{REMOTE_ADDR},setvar:ip.requests=
+1,expirevar:ip.requests=1"

# si hay más de 5 solicitudes por segundo por IP# bloqueo de
solicitudes var (expira en 5 segundos) y el aumento de
solicitudes var por IP (expira en una hora)
SecRule ip:requests "@eq 5"
"phase:1,pass,nolog,setvar:ip.block=1,expirevar:ip.block=5,setvar
:ip.blocks=+1,expirevar:ip.blocks=3
600"

# si el usuario es bloqueado más de 5 veces (var blocks>5), se
genera un log y se envía la petición a http 403
SecRule ip:blocks "@ge 5" "phase:1,deny,log,logdata:'req/sec:
%{ip.requests}, blocks: %{ip.blocks}',status:403"

# si el usuario es bloqueado (var block=1), se genera un log y se
envía la petición a http 403
SecRule ip:block "@eq 1" "phase:1,deny,log,logdata:'req/sec:
%{ip.requests}, blocks: %{ip.blocks}',status:403"

# 403 con mensaje de error
ErrorDocument 403 "<center><h2>Ha sido bloqueado por ataque!"
```

Figura 26 Listado de reglas que bloquean ataques del tipo DoS o DdoS

Para que el servidor apache pueda ejecutar las reglas de filtrado se debe reiniciar.

```
[root@leon:~] /etc/init.d/apache2 restart
```

Figura 27 Reinicio de apache

Luego de lo anterior, se procede a la realización del ataque tal como se indicó anteriormente con la herramienta Http attack versión 3.6.

El resultado es que el servidor apache bloquea por completo a la dirección ip atacante.

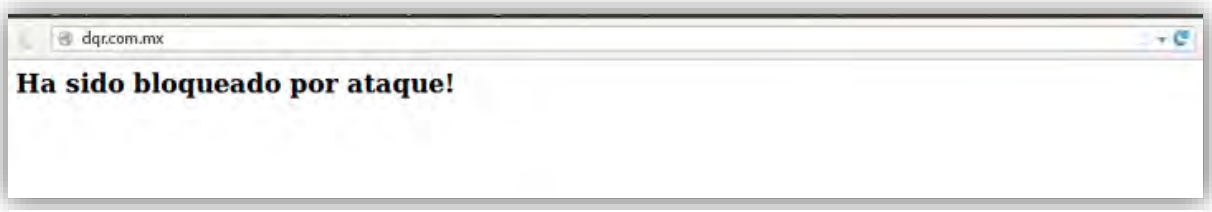


Figura 28 Resultado del bloqueo

Conclusiones

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 intensos, 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.

Por otro lado el apache mod security puede bloquear distintos ataques hacia las aplicaciones web alojadas en el servidor, filtra no solo el puerto 80 sino también el 443. Es importante agregar que “Provee protección contra las principales amenazas del Top 10 de **OWASP** (Open Web Application Security) mediante su conjunto de reglas especializadas en detección y bloqueo de ataques. Es un proyecto con madurez de desarrollo y cuenta con una creciente comunidad de usuarios que lo han implementado”. (13) Lo que abre paso a la posibilidad de realizar en el futuro nuevos estudios sobre el rendimiento de distintas reglas de mitigación de otros tipos de ataques con la ayuda de este WAF.

La implementación de una política de monitoreo para utilizar la herramienta netstat diariamente de 9am-12pm es muy necesaria, pues el administrador de red deberá analizar el tráfico para determinar si alguna dirección es un atacante, a fin de agregar a la lista negra del firewall las direcciones IP que resulten muy sospechosas. Este análisis debe ser realizado por el administrador de la red, quien puede determinar cuáles direcciones IP generan un tráfico legítimo y quienes resultan ser atacantes.

Tras la implementación de las herramientas de seguridad, los ataques posteriormente registrados en el servidor no surtieron efecto. Al parecer las medidas de mitigación cumplieron con el objetivo, sin embargo, en caso de que el o los

atacantes se organizaran para realizar un ataque DDoS más complejo, todavía existe una gran posibilidad de que el servidor web deje de estar disponible para los usuarios genuinos. Tras dicha posibilidad, se puede acudir a empresas especializadas que proporcionan servicio de soporte de seguridad ante ataques masivos del tipo DDos, pues es lo que más le convendría a la empresa del Diario de Quintana Roo ante la falta de recursos económicos para hacerse de la infraestructura necesaria para garantizar la completa eliminación de esta vulnerabilidad, aunque definitivamente cuenta con mayor seguridad y estabilidad que antes de la implementación de las herramientas de mitigación de ataques DDoS descritas en este trabajo, con la consecuente mejora económica, pues los clientes confían más en la disponibilidad del servicio publicitario que han adquirido en la aplicación web del Diario de Quintana Roo, lo que los hace estar dispuestos a volver a adquirirlos en futuras ocasiones y hasta recomendarlos a familiares o amigos.

Ahora recomendaría que se tomen medidas para prevenir otro tipo de ataques como el de password sniffing, todos los derivados del Cross site scripting etc. Utilizando la herramienta WAF Apache Mod Security. Actualmente el servidor se encuentra trabajando de forma estable, utilizando las herramientas descritas anteriormente y ya se ha contactado con una empresa prestadora de servicios de seguridad anti DDoS.

Anexo A

Resumen del archivo mod_evasive20.so

Resumen del archivo mod_evasive20.so. Codigo en el que básicamente se realiza la función del bloqueo de las direcciones IP atacantes.

Tabla 1 Archivo mod_evasive20.so

```
.
.
.
/* BEGIN DoS Evasive Maneuvers Definitions */

#define MAILER  "/bin/mail %s"
#define  LOG( A, ... ) { openlog("mod_evasive", LOG_PID,
LOG_DAEMON); syslog( A, __VA_ARGS__ ); closelog(); }

#define DEFAULT_HASH_TBL_SIZE   3097ul  // Default hash table
size
#define DEFAULT_PAGE_COUNT      2       // Default maximum page
hit count per interval
#define DEFAULT_SITE_COUNT      50      // Default maximum site
hit count per interval
#define DEFAULT_PAGE_INTERVAL   1       // Default 1 Second page
interval
#define DEFAULT_SITE_INTERVAL   1       // Default 1 Second site
interval
#define DEFAULT_BLOCKING_PERIOD 10      // Default for Detected
IPs; blocked for 10 seconds
#define DEFAULT_LOG_DIR         "/tmp"  // Default temp
directory

/* END DoS Evasive Maneuvers Definitions */

/* BEGIN NTT (Named Timestamp Tree) Headers */

enum { ntt_num_primes = 28 };

/* ntt root tree */
struct ntt {
    long size;
    long items;
    struct ntt_node **tbl;
};

/* ntt node (entry in the ntt root tree) */
struct ntt_node {
    char *key;
    time_t timestamp;
    long count;
    struct ntt_node *next;
```

```
};

/* ntt cursor */
struct ntt_c {
  long iter_index;
  struct ntt_node *iter_next;
};

struct ntt *ntt_create(long size);
int ntt_destroy(struct ntt *ntt);
struct ntt_node *ntt_find(struct ntt *ntt, const char *key);
struct ntt_node *ntt_insert(struct ntt *ntt, const char *key,
time_t timestamp);
int ntt_delete(struct ntt *ntt, const char *key);
long ntt_hashcode(struct ntt *ntt, const char *key);
struct ntt_node *c_ntt_first(struct ntt *ntt, struct ntt_c *c);
struct ntt_node *c_ntt_next(struct ntt *ntt, struct ntt_c *c);

/* END NTT (Named Timestamp Tree) Headers */


/* BEGIN DoS Evasive Maneuvers Globals */

struct ntt *hit_list; // Our dynamic hash table

# Declaración de variables, que permitirán obtener valores
necesarios para realizar la evasión de los ataques
static unsigned long hash_table_size = DEFAULT_HASH_TBL_SIZE;
static int page_count = DEFAULT_PAGE_COUNT;
static int page_interval = DEFAULT_PAGE_INTERVAL;
static int site_count = DEFAULT_SITE_COUNT;
static int site_interval = DEFAULT_SITE_INTERVAL;
static int blocking_period = DEFAULT_BLOCKING_PERIOD;
static char *email_notify = NULL;
static char *log_dir = NULL;
static char *system_command = NULL;
static const char *whitelist(cmd_parms *cmd, void *dconfig,
const char *ip);
int is_whitelisted(const char *ip);

/* END DoS Evasive Maneuvers Globals */

static void * create_hit_list(apr_pool_t *p, server_rec *s)
{
    /* Create a new hit list for this listener */

    hit_list = ntt_create(hash_table_size);
}

static const char *whitelist(cmd_parms *cmd, void *dconfig,
const char *ip)
```

```
{
  char entry[128];
  snprintf(entry, sizeof(entry), "WHITELIST_%s", ip);
  ntt_insert(hit_list, entry, time(NULL));

  return NULL;
}


static int access_checker(request_rec *r)
{
    int ret = OK;
#A partir de aquí inician las maniobras evasivas
    /* BEGIN DoS Evasive Maneuvers Code */

    if (r->prev == NULL && r->main == NULL && hit_list != NULL)
{
      char hash_key[2048];
      struct ntt_node *n;
      time_t t = time(NULL);
#Busca a la ip atacante dentro de una lista blanca que se puede
definir en el archivo mod_evasive.conf
      /* Check whitelist */
      if (is_whitelisted(r->connection->remote_ip))
        return OK;
#Mantiene la dirección ip en el tiempo de espera definido el
archive mod_evasive.conf
      /* First see if the IP itself is on "hold" */
      n = ntt_find(hit_list, r->connection->remote_ip);

      if (n != NULL && t-n->timestamp<blocking_period) {
#Si está en espera, la mantienen más tiempo bloqueada
        /* If the IP is on "hold", make it wait longer in 403
land */
        ret = HTTP_FORBIDDEN;
        n->timestamp = time(NULL);

      /* Not on hold, check hit stats */
      } else {

        /* Has URI been hit too much? */
        snprintf(hash_key, 2048, "%s_%s", r->connection-
>remote_ip, r->uri);
        n = ntt_find(hit_list, hash_key);
        if (n != NULL) {
#Si esa dirección está atacando a un recurso por demasiado
tiempo, la añade automáticamente a la lista de IP bloqueadas
          /* If URI is being hit too much, add to "hold" list
and 403 */
          if (t-n->timestamp<page_interval && n-
>count>=page_count) {
```

```
            ret = HTTP_FORBIDDEN;
            ntt_insert(hit_list, r->connection->remote_ip,
time(NULL));
          } else {

            /* Reset our hit count list as necessary */
            if (t-n->timestamp>=page_interval) {
              n->count=0;
            }
          }
          n->timestamp = t;
          n->count++;
        } else {
          ntt_insert(hit_list, hash_key, t);
        }
# Si esa dirección está atacando a un sitio por demasiado
tiempo, la añade automáticamente a la lista de IP bloqueadas
        /* Has site been hit too much? */
        snprintf(hash_key, 2048, "%s_SITE", r->connection-
>remote_ip);
        n = ntt_find(hit_list, hash_key);
        if (n != NULL) {

          /* If site is being hit too much, add to "hold" list
and 403 */
          if (t-n->timestamp<site_interval && n-
>count>=site_count) {
            ret = HTTP_FORBIDDEN;
            ntt_insert(hit_list, r->connection->remote_ip,
time(NULL));
          } else {

            /* Reset our hit count list as necessary */
            if (t-n->timestamp>=site_interval) {
              n->count=0;
            }
          }
          n->timestamp = t;
          n->count++;
        } else {
          ntt_insert(hit_list, hash_key, t);
        }
      }
# Realiza la estructura de un e-mail y lo envía que notificará
la dirección IP bloqueada y crea un archivo log, para su
posterior consulta.
      /* Perform email notification and system functions */
      if (ret == HTTP_FORBIDDEN) {
        char filename[1024];
        struct stat s;
        FILE *file;
```

```
        snprintf(filename, sizeof(filename), "%s/dos-%s",
log_dir != NULL ? log_dir : DEFAULT_LOG_DIR, r->connection-
>remote_ip);
        if (stat(filename, &s)) {
          file = fopen(filename, "w");
          if (file != NULL) {
            fprintf(file, "%ld\n", getpid());
            fclose(file);
            LOG(LOG_ALERT, "Blacklisting address %s: possible
DoS attack.", r->connection->remote_ip);
            if (email_notify != NULL) {
              snprintf(filename, sizeof(filename), MAILER,
email_notify);
              file = popen(filename, "w");
              if (file != NULL) {
                fprintf(file, "To: %s\n", email_notify);
                fprintf(file, "Subject: HTTP BLACKLIST %s\n\n",
r->connection->remote_ip);
                fprintf(file, "mod_evasive HTTP Blacklisted
%s\n", r->connection->remote_ip);
                pclose(file);
              }
            }

            if (system_command != NULL) {
              snprintf(filename, sizeof(filename),
system_command, r->connection->remote_ip);
              system(filename);
            }

          } else {
            LOG(LOG_ALERT, "Couldn't open logfile %s:
%s",filename, strerror(errno));
        }

        } /* if (temp file does not exist) */

      } /* if (ret == HTTP_FORBIDDEN) */

    } /* if (r->prev == NULL && r->main == NULL && hit_list !=
NULL) */
#concluyen las maniobras evasivas.
    /* END DoS Evasive Maneuvers Code */

.
.
.
```

Anexo B

Contenido del script perl para probar el apache mod_evasive

Contenido del script perl para probar el apache mod_evasive.

```
#!/usr/bin/perl

# test.pl: small script to test mod_dosevasive's effectiveness

use IO::Socket;
use strict;
 # Mediante un ciclo se realizan de 0 a 100 peticiones a través
del protocolo TCP al puerto 80
for(0..100) {
  my($response);
  my($SOCKET) = new IO::Socket::INET( Proto   => "tcp"
PeerAddr=> "target.com:80");
# Se imprime la respuesta a las peticiones realizadas al servidor
if (! defined $SOCKET) { die $!; }
  print $SOCKET "GET /?$_ HTTP/1.0\n\n";
  $response = <$SOCKET>;
  print $response;
  close($SOCKET);
}
```

Figura 29 Script perl para probar el apache mod_evasive

Bibliografía

1. **Anónimo.** *Linux Máxima Seguridad.* [trad.] S.L. José Arroyo Traducciones Vox Populi. California : Prentice Hall.

2. **Shreves, Ric.** *Joomla! Bible.* [ed.] Beth Taylor. Indianapoli : Wiley Publishing, Inc., 2010.

3. **Egea, Fracisco Javier.** *Servidores para Internet con Apache HttpServer.* Madrid : Grupo EIDOS Consultaría y Documentación Informática, S.L., 2000, 2008.

4. **Kabir, Mohammed J.** *La biblia de Servidor Apache.* Madrid : Ediciones Anaya Multimedia (Grupo Anaya, S.A.), 2003.

5. **Zdziarski, Jonathan.** zdziarski.com. *zdziarski.com.* [En línea] 14 de marzo de 2010. [Citado el: 10 de abril de 2011.] http://www.zdziarski.com/blog/?page_id=442.

6. **Trustwave.** modsecurity Open Source Web Aplication Firewall. [En línea] [Citado el: 18 de abril de 2011.] http://www.modsecurity.org/.

7. **Notimex.** excelsior. [En línea] Periódico Excélsior, S.A. de C.V, 09 de diciembre de 2010. [Citado el: 27 de abril de 2011.] http://www.excelsior.com.mx/index.php?m=nota&id_nota=695316.

8. **Roo, Departamento de Computo y Telemática del Diario de Quintana.** 16 de agosto de 2010.

9. **Netstat Systems.** Netstat Systems. *Netstat Systems.* [En línea] [Citado el: 28 de diciembre de 2010.] http://www.netstat.net/.

10. **The Nagios Team.** Nagios. [En línea] Nagios Enterprises, LLC, 2009. [Citado el: 27 de abril de 2011.] http://www.nagios.org.

11. **Méndez, Sayonara Sarahí Díaz.** Seguridad Cultura de Prevención Para TI. [En línea] 05 de marzo de 2013. [Citado el: 18 de agosto de 2013.] http://revista.seguridad.unam.mx/numero-16/firewall-de-aplicaci%C3%B3n-web-parte-i. 16.

12. **ModSecurityProyect.** modsecurity. *modsecurity.* [En línea] Trustwave, junio de 2009. [Citado el: 31 de agosto de 2011.] http://www.modsecurity.org/documentation/modsecurity-apache/2.1.2/modsecurity2-apache-reference.html#N10311.

13. **Sayonara Sarahí Díaz Méndez, Dante Odín Ramírez López.** Seguridad Cultura de Prevención para las TI. [En línea] Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, 2 de mayo de 2013. [Citado el: 25 de agosto de 2013.] http://revista.seguridad.unam.mx/numero-17/firewall-de-aplicaci%C3%B3n-web-parte-ii. 17.