Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VII Número: Edición Especial Artículo no.:27 Período: Abril, 2020

TÍTULO: Evaluación de ataques DDoS y fuerza bruta utilizando entorno virtual Kali Linux como plataforma experimental.

AUTORES:

1. Máster. Edgar Fabricio Rivera Osorio.
2. Máster. Miriam Patricia Cárdenas Zea.
3. Máster. Washington Alberto Chiriboga Casanova.

RESUMEN: La investigación se enfoca en la evaluación de ataques de denegación de servicios tipo SYN Flood y ataques de fuerza bruta, utilizando como plataforma de experimentación un entorno virtual de red que permita identificar cómo actúan dichos ataques en la saturación del ancho de banda y descubrir la contraseña del usuario administrador para poder ingresar a un sitio web con fines maliciosos. Para validar está investigación se desarrolló un mecanismo de detección y mitigación de los ataques en los hosts víctimas, a nivel de la capa de Internet del modelo TCP/IP con la formulación de reglas a nivel del firewall Iptables en Linux Centos 6.7.

PALABRAS CLAVES: ataque de seguridad, virtualización, Kali Linux, fuerza bruta, DDoS.

TITLE: DDoS and brute force evaluation using Kali Linux virtual environment as an experimental platform.

AUTHORS:

1. Master. Edgar Fabricio Rivera Osorio.
2. Master. Miriam Patricia Cárdenas Zea.
3. Master. Washington Alberto Chiriboga Casanova.

ABSTRACT: The research focuses on the evaluation of denial of service attacks like SYN Flood and brute force attacks, using a virtual network environment as an experimentation platform to identify how these attacks act in bandwidth saturation and discover the password. of the administrator user to be able to enter a website for malicious purposes. To validate this research, a mechanism for detecting and mitigating attacks on victim hosts was developed, at the Internet layer level of the TCP / IP model with the formulation of rules at the level of the Iptables firewall in Linux Centos 6.7.

KEY WORDS: Security Attack, Virtualization, Kali Linux, Brute Force, DDoS.

INTRODUCCIÓN.

En los últimos años, los ataques e intrusiones han causado pérdidas no solo económicas, sino que han afectado la imagen, credibilidad y competitividad de los sistemas afectados generando incertidumbre por los riesgos que día a día están expuestos como: modificación, interrupción, falsificación, denegación de servicios, etc.

Para prevenir y contrarrestar una amplia gama de amenazas en una red de comunicaciones, es necesario conocer sus vulnerabilidades e identificar diversos tipos de ataques. Para manejar esta situación se propone crear un ambiente de red controlado con los componentes necesarios que detecten ataques maliciosos, para analizarlos y contrarrestarlos. Una primera alternativa sería mediante equipos reales; sin embargo, esto encarecería la solución y pondría en riesgo la red en producción. Otra alternativa sería utilizar máquinas virtuales, con las cuales es posible reducir costos de inversión de hardware, costos de mantenimiento, costo y tiempo de experimentación y sobre todo

reduciría el riesgo del colapso de la red en producción (Fuertes. W, J. E. L. de Vergara, and F. Meneses, 2009).

Sobre la base de las consideraciones anteriores para esta investigación se seleccionó un ataque de Denegación de Servicio (Denial of Service -DoS-) mediante la herramienta Metasploit y un ataque de fuerza bruta mediante WPScan hacia dos clientes en un ambiente virtualizado mediante la utilización de la plataforma Kali Linux con lo que se demostró las vulnerabilidades existentes dentro de los entornos elegidos como víctimas.

Un ataque de Denegación de Servicio (Denial of Service -DoS-) tiene el propósito de evitar que el usuario legítimo haga uso de un recurso o servicio específico de red o un host. Entre las variantes de este tipo de ataque se pueden citar la inundación de la red mediante la inyección de paquetes, consumiendo el ancho de banda; la inanición de recursos, saturando la memoria; los errores de programación, para colapsar el procesador, y los ataques DNS y enrutamiento, para convencer mediante direcciones falsas y suplantación de identidad (Fuentes W, F. Rodas, and D. Toscano., 2011).

Un ataque por fuerza bruta se basa en la formación de palabras mediante combinación de caracteres hasta encontrar una que coincida con la contraseña protectora (Zapata Molina. 2012).

La comunidad científica ha investigado tratando de implementar soluciones para disminuir y mitigar los ataques basados en las vulnerabilidades de los sistemas, por tal motivo, ha planteado soluciones basadas en las tecnologías de virtualización para con ello disminuir el riesgo en equipos y redes de producción.

Los trabajos propuestos por Fuertes et al. (2011) presentan una evaluación de ataques DoS utilizando como plataforma de experimentación un entorno virtual de red que permita identificar cómo actúan dichos ataques en la saturación del ancho de banda y cuál sería su impacto.

El trabajo propuesto por Mukhopadhyay, Goswami y Mandal et al. [4] muestra la penetración web utilizando una arquitectura virtualizada mediante la herramienta Metasploit para validar las vulnerabilidades de exploración de un sitio web. Narváez Portillo et al. (2011) presenta una metodología de análisis de detección de intrusiones mediante la plataforma Kali Linux con la cual se puede determinar las vulnerabilidades, severidad y consecuencias.

El trabajo propuesto por Molina et al. [3] expone diferentes ataques entre ellos, ataques de fuerza bruta, suplantación de identidad y denegación de servicios, utilizando un entorno virtualizado con software libre tanto para producir el ataque como para obtener el flujo de tráfico, evaluando las consecuencias obtenidas. Según (Méndez S. S. D. and D. O. R. López. 2013). Un WAF trabaja como intermediario entre usuarios externos (ej. usuarios de Internet) y las aplicaciones web. Esto quiere decir que las peticiones y respuestas HTTP son analizadas por el WAF antes de que éstas lleguen a las aplicaciones web o a los usuarios de las aplicaciones.

El presente trabajo se enfoca en la evaluación de ataques de DDoS y fuerza bruta utilizando el entorno virtual Kali Linux como plataforma experimental. Para llevarlo a cabo se diseñó e implementó una red virtual con el propósito de inhabilitar el acceso interno y externo a un servicio Web expuesto. Las herramientas evaluadas fueron Metasploit (OffSec Services Limited 2020) y WPScan (The WPScan Team 2020) instaladas sobre el ambiente virtualizado. Para validar esta investigación se desarrolló un mecanismo de detección y mitigación de ataques a nivel de iptables y la implementación de un WAF, evitando el acceso y saturación de la red.

Entre las principales contribuciones de esta investigación cabe mencionar: i) la evaluación de ataques DDoS y Fuerza Bruta, ii) creación de reglas a nivel de iptables que permitan la detección y mitigación de ataques a nivel de la capa de Internet, iii) instalación e implementación de un Web Aplication Firewall que permita la detección y mitigación de ataques a nivel de la capa de aplicación, y iv) evaluación de ataques utilizando entorno Virtual Kali Linux.

El documento ha sido organizado de la siguiente manera: en la sección 2 encontraremos algunos fundamentos teóricos, en la sección 3 una breve explicación de la configuración del experimento, en la sección 4 se presenta, analizan y evalúan los resultados, en la sección 5 se encontrarán los trabajos relacionados y en la sección 6 se establece el análisis de conclusiones y trabajos futuros.

DESARROLLO.

Fundamento teórico.

Virtualización.

Según (Ordoñez Pacheco, 2009), la virtualización consiste en una capa abstracta que permite que múltiples máquinas virtuales con sistemas operativos (SO) heterogéneos puedan ejecutarse individualmente, operando en la misma máquina física.

Escenario virtual de red.

De acuerdo al criterio de (Zapata Molina, 2012), un escenario virtual de red puede ser definido como un conjunto de equipos virtuales (tanto sistemas finales como elementos de red (enrutadores y conmutadores) conectados entre sí en una determina topología, cuyo entorno deberá ser percibido como si fuera real.

Denegación del servicio.

Acorde al autor (Zapata Molina. 2012), son ataques que provocan que un servicio, equipo o recurso sea inaccesible para usuarios legítimos. Para esto se envía mensajes TCP de petición de conexión por parte del cliente, pero sin enviar su confirmación lo cual provoca colapsos en equipos y consumo de recursos en forma desproporcionada, muchas veces la dirección de origen es falsificada

Ataque de Fuerza Bruta.

Este método se basa en la formación de palabras mediante combinación de caracteres hasta encontrar una que coincida con la contraseña protectora. (Zapata Molina. 2012).

Configuración del experimento.

Herramientas.

En este experimento se utilizó herramientas de código abierto y de libre distribución; a continuación, se detallan:

1) Sistema de Virtualización: Como plataforma de virtualización se utilizó VMware Workstation sobre Kali Linux y Centos 6.7 en dos hosts anfitrión. Su objetivo fue configurar múltiples computadoras interconectadas mediante un switch que luego fue conectado a otro pc virtual que simuló la función de un router para poder enrutar el tráfico y tener salida hacia internet.
2) Firewall en capa de Internet: Como firewall a nivel de la capa de Internet, se utilizó iptables en Linux Centos 6.7; Su objetivo es disponer de un cortafuego que permita establecer seguridad entre zonas de confianza como LAN y DMZ. Los iptables permiten o niegan el tráfico desde una ip con puerto origen hacia una ip con puerto destino controlando y mitigando ataques hacia los recursos de la red.
3) Firewall en capa de Aplicación: Como firewall a nivel de la capa de Aplicación, se utilizó el Web Aplication Firewall (WAF) Mod-security en Linux Centos 6.7, el cual se ejecuta como módulo del servidor web Apache, proporcionando protección contra diversos ataques hacia aplicaciones Web y permitiendo monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente. Este módulo tiene las siguientes funcionalidades: i) Filtrado de Peticiones: los pedidos HTTP entrantes son analizados por el módulo Mod-security antes de pasarlos al servidor Web Apache, a su vez, estos pedidos son

comparados contra un conjunto de reglas predefinidas para realizar las acciones correspondientes. Para realizar este filtrado se pueden utilizar expresiones regulares, permitiendo que el proceso sea flexible; ii) Técnicas anti evasión: las rutas y los parámetros son normalizados antes del análisis para evitar técnicas de evasión: elimina múltiple barras (//), elimina directorios referenciados por si mismos (**./**), trata de igual manera la \ y la **/** en Windows, decodifica URL y reemplaza bytes nulos por espacios (**%00**); iii) Comprensión del protocolo HTTP: al comprender el protocolo HTTP, Mod-security puede realizar filtrados específicos y granulares; iv) Análisis Post Payload: intercepta y analiza el contenido transmitido a través del método POST; v) Log de Auditoría: es posible dejar traza de auditoría para un posterior análisis forense; vi) Filtrado HTTPS: al estar embebido como módulo, tiene acceso a los datos después de que estos hayan sido descifrados; vii) Verificación de rango de Byte: permite detectar y bloquear shellcodes, limitando el rango de los bytes.

4) Web Server: Como servidor Web se utilizó Apache sobre Linux Centos 6.7; su objetivo fue servir una página Web programada con Wordpress, php y una base de datos en Mysql para el almacenamiento de usuarios y contraseñas solicitada por equipos clientes mediante el uso de navegadores Web, que luego sería víctima de ataques de DDoS y fuerza bruta.
5) Herramienta para DDoS: Como herramienta de DDoS se utilizó Metasploit. Su objetivo fue realizar inundación de paquetes SYN Flood al host donde está alojado el sitio web e impedir su acceso por los usuarios legítimos.
6) Herramienta para Ataque de Fuerza Bruta: Como herramienta para realizar el ataque de fuerza bruta se utilizó WPScan. Su objetivo es atacar al sitio web creado con wordpress para tratar de encontrar las contraseñas de los usuarios almacenadas en la base de datos Mysql alojada en el host víctima y poder tener un acceso no autorizado y violentar los datos.

7) Captura de Trafico: Como herramientas para captura de tráfico se utilizó IPTraf y Wireshark sobre el Linux Centos 6.7 que tiene configurado el firewall iptables y el Web Server Apache respectivamente; su objetivo fue identificar y analizar el tráfico que circula por la red, analizar los paquetes de datos en el host víctima antes y después de la mitigación de los ataques generados.

Diseño de la topología experimental.

La generación de ataques de Fuerza bruta con WPScan, Denegación de Servicios, DDoS, utilizando Metasploit, y su mecanismo de mitigación requirieron de la creación de una infraestructura de red similar a la utilizada por cualquier red en producción. Es así que para el diseño e implementación de la topología de prueba se requirió de un enrutador que posibilitó la salida a Internet, un computador con Kali Linux (atacante externo) y un equipo anfitrión de Virtualización que permitió crear los diferentes componentes de la implementación con VMware y Linux Centos 6.7, convirtiéndola en una plataforma híbrida, tal como se muestra en la Fig. 1.

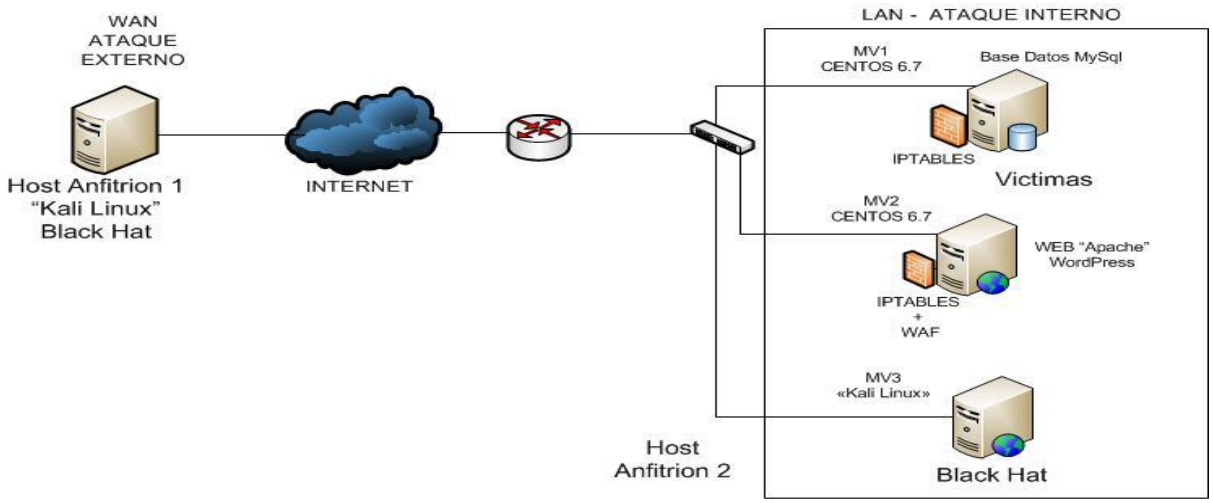

Fig. 1. Diseño para la generación y mitigación de ataques de fuerza bruta y DDoS.

Implementación de la Plataforma Experimental.

Las pruebas de ataque se ejecutaron desde un equipo anfitrión VMware, bajo Windows7, con procesador Core7, memoria 8Gb y almacenamiento 1 Tb. En esta máquina virtual se instaló Kali

Linux con las herramientas WPScan, Nmap y Metasploit. En otro equipo anfitrión de similares características con VMware bajo Windows7, se instalaron tres máquinas Virtuales con Linux Centos 6.7 (hosts víctimas) donde se instalaron la base de datos MySql y el Servidor Web Apache y una atacante interno con Kali Linux. En estas máquinas virtuales con Linux Centos 6.7 fueron configuradas las reglas a nivel de firewall Iptables y el módulo Mod-security para mitigar los ataques generados.

El siguiente procedimiento ha sido utilizado para implementar el diseño propuesto en un entorno virtual: i) En primer lugar, se ha sincronizado el reloj mediante el protocolo de temporización de red (NTP) en los equipos anfitriones; ii) Luego se ha creado la primera máquina virtual VMware, en la cual se ha instalado el sistema operativo Kali Linux para realizar los ataques desde la WAN; iii) Posteriormente, en otro host anfitrión se ha creado dos máquinas virtuales VMware, en la cual se ha instalado el sistema operativo Linux Centos 6.7 con Web Server Apache y el módulo Mod-security en una y en la otra con la base de datos Mysql respectivamente IV) A continuación, se creó una tercera máquina virtual con VMware donde se instaló Kali Linux. Adicionalmente, se instaló WPScan, Nmap y Metasploit para escanear puertos y generar ataques desde la LAN. En este punto, cabe señalar, que el enrutador y el switch de la Fig. 1 son dispositivos físicos que conectan al equipo anfitrión tanto hacia el Internet como a las máquinas virtuales.

Configuración del firewall.

Para mitigar el ataque de fuerza bruta realizado contra el Host víctima que contenía la base de datos MySql, se formularon reglas a nivel de firewall en Linux Centos 6.7, tal como se muestra en la Fig. 2.

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp -s 192.168.145.131 --dport 3306 -j R
EJECT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A OUTPUT -m comment --comment "Permitir conexiones salientes " -j ACCEPT
-A FORWARD -m comment --comment "Permitir conexiones forward " -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
~
~
~
"/etc/sysconfig/iptables" 17L, 774C                          11,1          All
```

Fig. 2. Reglas a nivel de firewall Iptables en Linux Centos 6.7 para mitigar ataques de fuerza bruta.

Para mitigar el ataque de DDoS realizado contra el Servidor Web Apache, se formularon reglas a nivel de firewall Iptables en Linux Centos 6.7, tal como se muestra en la Fig. 3.

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
#-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j REJECT
#-A INPUT -m state --state NEW -m tcp -p tcp -s 192.168.145.134 --dport 22 -j REJECT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name puerto_22 --set -m comment --comment "Inicio filtrado 22 "
-A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name puerto_22 --update --seconds 3600 --hitcount 5 -j LOG --log-prefix "Ataque DDO
-A INPUT -p tcp --dport 22 -m state --state NEW -m recent --name puerto_22 --update --seconds 3600 --hitcount 5 -j REJECT
-A INPUT -p tcp --dport 22 -m state --state NEW -m comment --comment "Fin filtrado 22 " -j ACCEPT
#Se están limitando los ataques usando el MATCH EXTENSION <93>limit<94>, a 1 conexión nueva por segundo
#y ráfagas de 5. Después de cada una de estas reglas hay otra que usa el TARGET EXTENSION <93>log<94>
#para logar los intentos de ataques DOS.
-A INPUT -p tcp --dport 80 -m state --state NEW -m limit --limit 1/second --limit-burst 5 -m comment --comment "Aceptar puerto 80" -j ACCEPT
-A INPUT -p tcp --dport 80 -m state --state NEW -m recent --name puerto_80 --set -m comment --comment "Inicio filtrado 80 "
-A INPUT -p tcp --dport 80 -m state --state NEW -m recent --name puerto_80 --update --seconds 60 --hitcount 30 -j LOG --log-prefix "Ataque DDOS
-A INPUT -p tcp --dport 80 -m state --state NEW -m recent --name puerto_80 --update --seconds 60 --hitcount 30 -j REJECT
-A INPUT -p tcp --dport 80 -m state --state NEW -m comment --comment "Fin filtrado 80 " -j ACCEPT
-A INPUT -p tcp --dport 443 -m state --state NEW -m recent --name puerto_443 --set -m comment --comment "Inicio filtrado 443 "
-A INPUT -p tcp --dport 443 -m state --state NEW -m recent --name puerto_443 --update --seconds 60 --hitcount 30 -j LOG --log-prefix "Ataque DD
"
-A INPUT -p tcp --dport 443 -m state --state NEW -m recent --name puerto_443 --update --seconds 60 --hitcount 30 -j REJECT
-A INPUT -p tcp --dport 443 -m state --state NEW -m comment --comment "Fin filtrado 443 " -j ACCEPT
-A OUTPUT -m comment --comment "Permitir conexiones salientes " -j ACCEPT
-A FORWARD -m comment --comment "Permitir conexiones forward " -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
```

Fig. 3. Reglas a nivel de firewall Iptables en Linux Centos 6.7 para mitigar ataques de DDoS SYN Flood.

Como las reglas a nivel de firewall Iptables solo bloquean el tráfico en la red a nivel de la capa de Internet del modelo TCP/IP, no aseguran una mitigación 100% segura contra ataques a aplicaciones Web, se instaló y configuró el módulo Mod-security sobre el servidor Apache activando las reglas bases y experimentales para realizar filtrado de peticiones HTTP y HTTPS y bloquear los ataques a nivel de capa de Aplicación contra el servicio Web, asegurando su disponibilidad a los usuarios, tal como se muestra en las Fig. 4, Fig. 5 y Fig. 6.

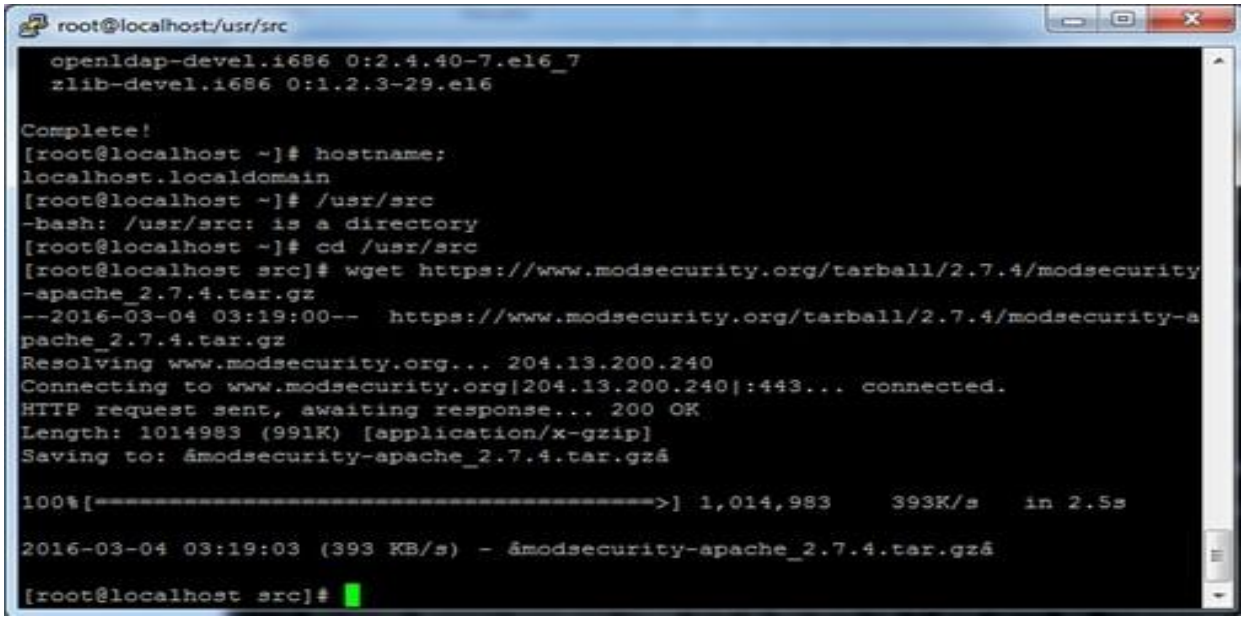

Fig. 4. Instalación del WAF Mod-security.

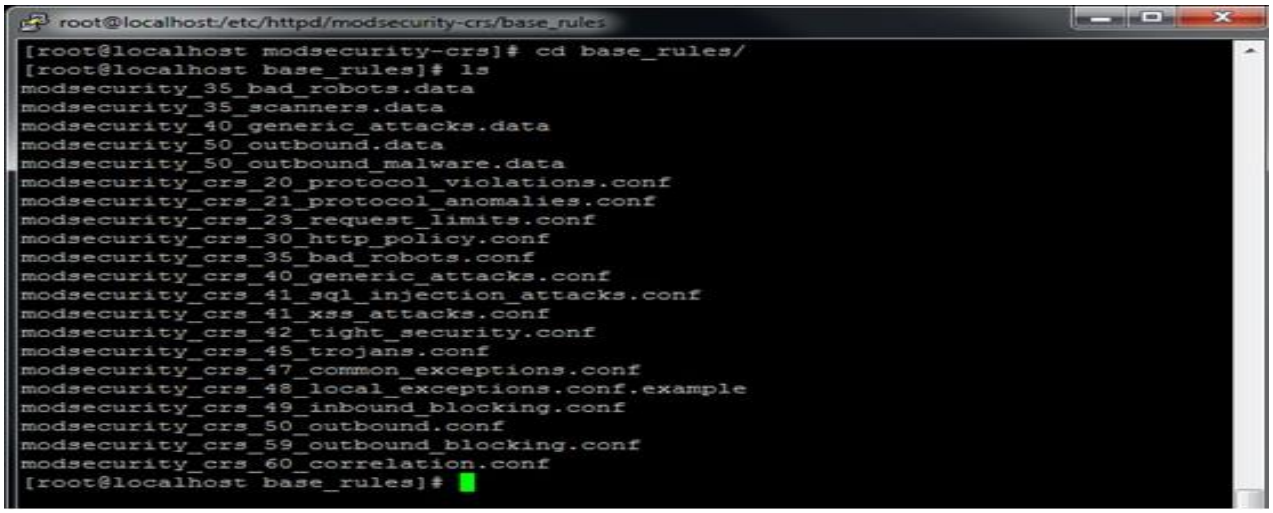

Fig. 5. Activación de reglas base del WAF Mod-security.

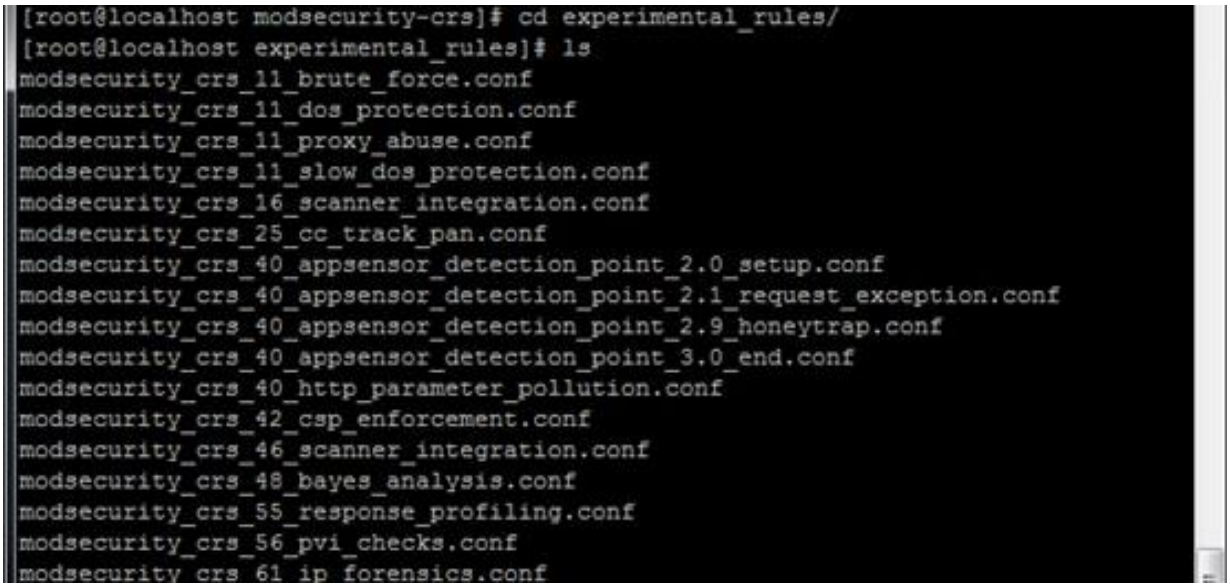

Fig. 6. Activación de reglas experimentales del WAF Mod-security**.**

Generación de ataques.

Con la debida configuración como un entorno real de las herramientas antes mencionadas y de una infraestructura de red similar a la utilizada por cualquier red en producción, se realizó la generación de ataques de DDoS, mediante la ejecución del programa Metasploit atacando interna como externamente, adicional se realizó un ataque de fuerza bruta ejecutando la herramienta WPScan a la ip del host donde se aloja la base de datos de usuarios y contraseñas creadas con Wordpress y almacenadas en Mysql, la cual realiza un matching de la posible contraseña con un diccionario de claves (wordlist) contenido en un archivo .txt, hasta descubrir la que permita el acceso no autorizado como administrador al sitio web, tal como se muestra en la Fig. 7.

Previamente, antes de realizar el ataque con WPScan, se realizó un escaneo de puertos con la herramienta Nmap para conocer si el puerto que utiliza la base de datos Mysql se encuentra abierto o no, tal como se muestra en la Fig. 8. El ataque de DDoS con Metasploit se caracterizó por generar un considerable volumen de tráfico en la red comprometiendo la disponibilidad del servicio web expuesto.

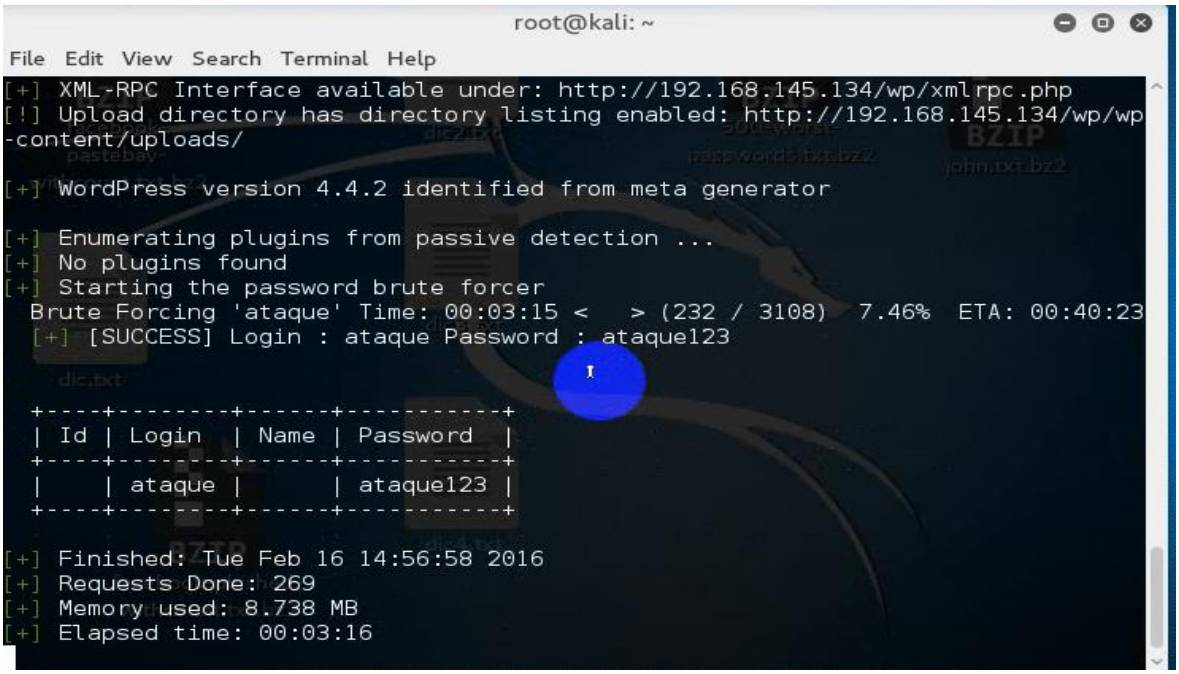

Fig. 7. Descubrimiento de contraseña de un usuario almacenada en la base de datos Mysql mediante la herramienta WPScan.

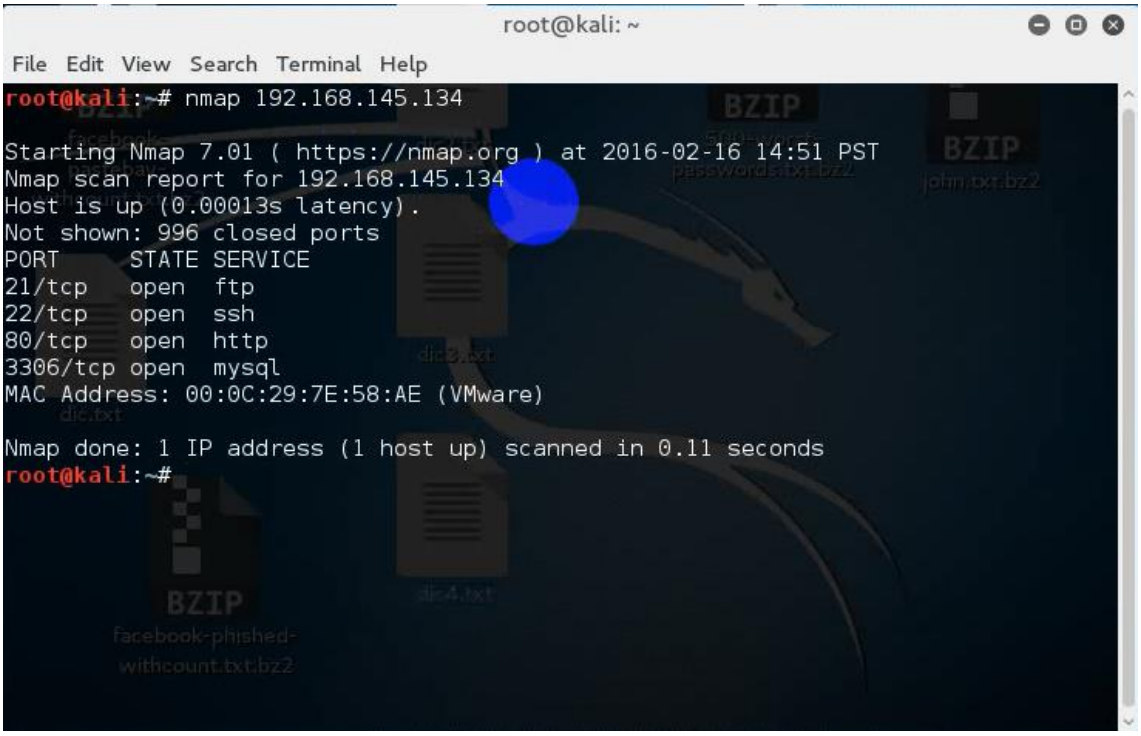

Fig. 8. Escaneo de puertos al host víctima mediante la herramienta Nmap.

Evaluación de resultados.

Los datos estadísticos obtenidos en los diferentes escenarios con las herramientas de monitoreo de tráfico IPTraf, Wireshark y el comando htop, tal como se muestra en Fig. 9 y Fig. 10, fueron evaluados teniendo como resultado el impacto en el consumo de memoria virtual, física y saturación de peticiones al momento de inundar la máquina víctima con ataques SYN Flood con la herramienta Metasploit.

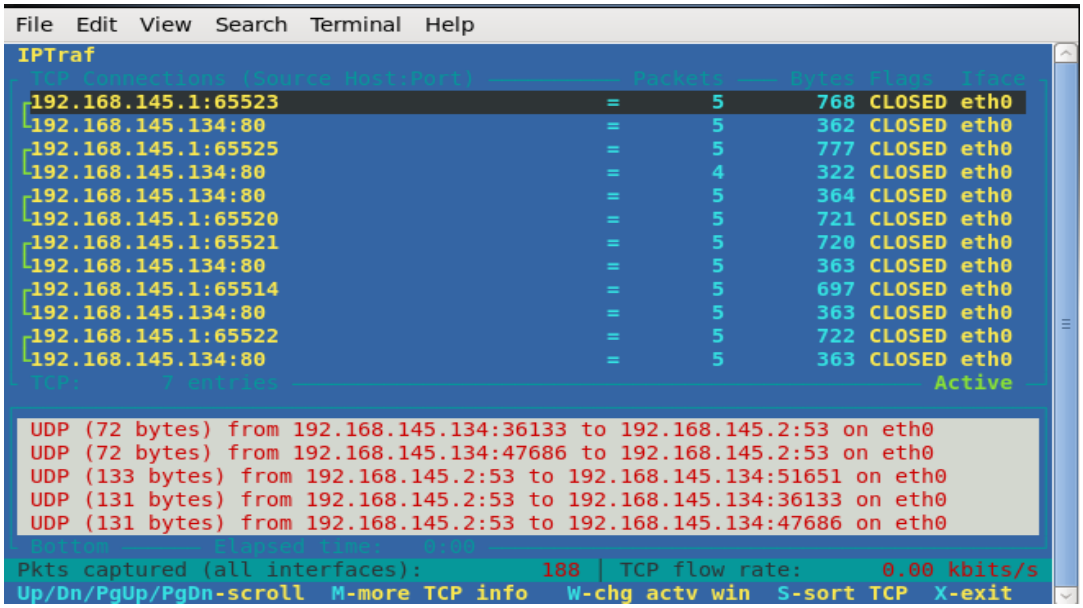

Fig. 9. Monitoreo de Ataque de DDoS SYN Flood Metasploit con IPTraf.

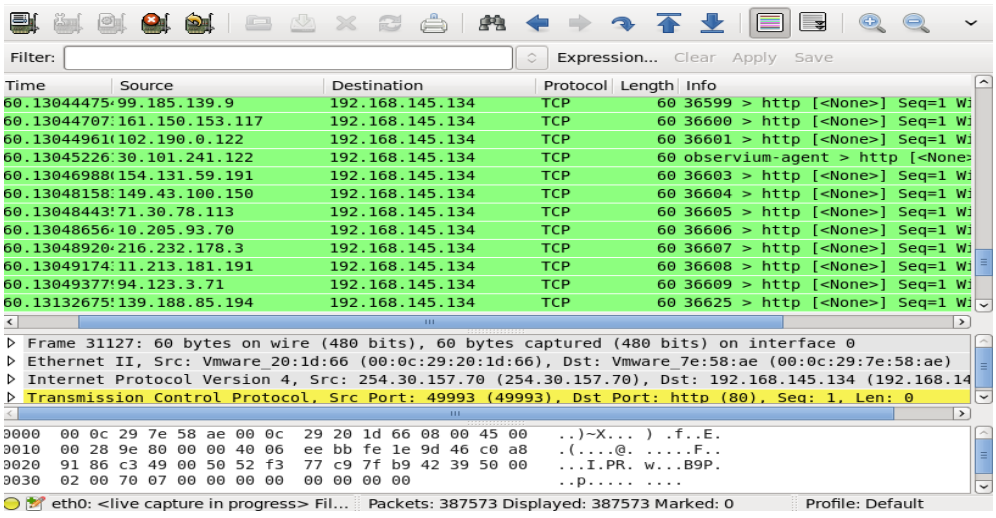

Fig. 10. Monitoreo de Ataque de DDoS SYN Flood Metasploit con Wireshark.

Aproximadamente, dos minutos después de realizado este ataque, el consumo de CPU del host víctima pasó del 14% al 100% y el consumo de memoria llegó hasta el 90%, tal como se muestra en la Fig. 11 y Fig. 12.

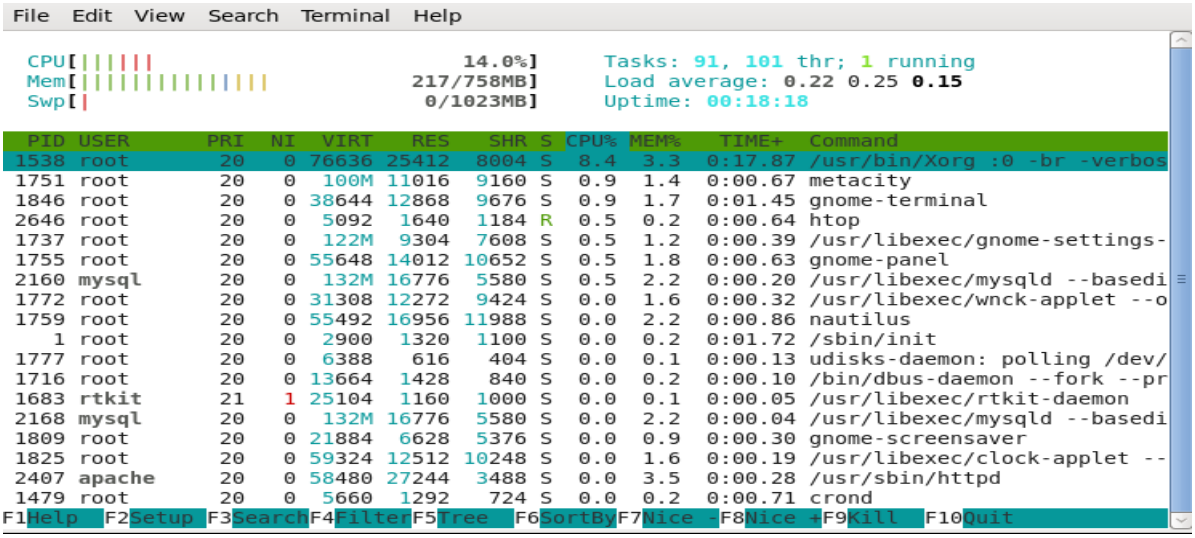

Fig. 11. Consumo de CPU y Memoria del host víctima antes del Ataque con Metasploit.

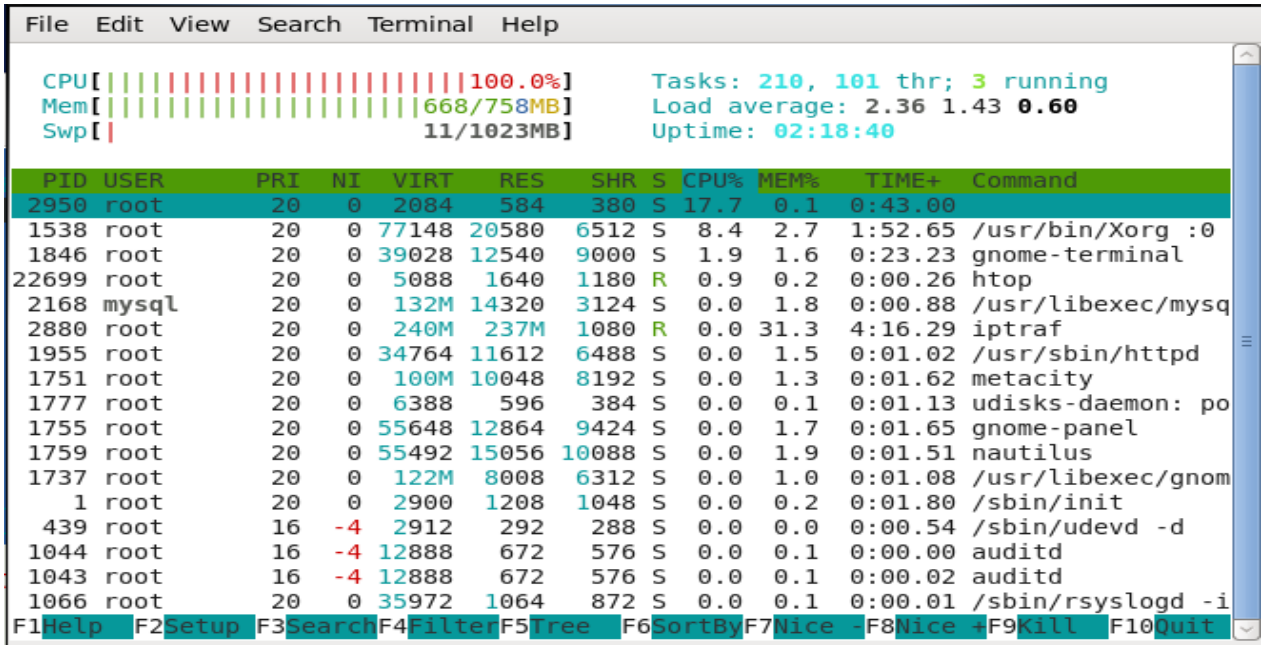

Fig. 12. Consumo de CPU y Memoria del host víctima durante el Ataque con Metasploit sin realizar mitigación con Iptables.

Después de realizado el ataque de DDoS con Metasploit se ejecutó el ataque de fuerza bruta mediante la herramienta WPScan, tanto interna (LAN) como externamente (WAN) al host víctima con la finalidad de descubrir la contraseña del usuario administrador y poder ingresar al sitio web con la finalidad de violentar los datos contenidos en la base Mysql. Cabe mencionar que el tiempo que tarda la herramienta WPScan en encontrar la contraseña es directamente proporcional al tamaño del Diccionario de Datos o wordlist contenido en el archivo .txt con el que realiza el matching, es decir se puede tardar minutos, horas, días hasta semanas, tal como se muestra en la Fig. 13.

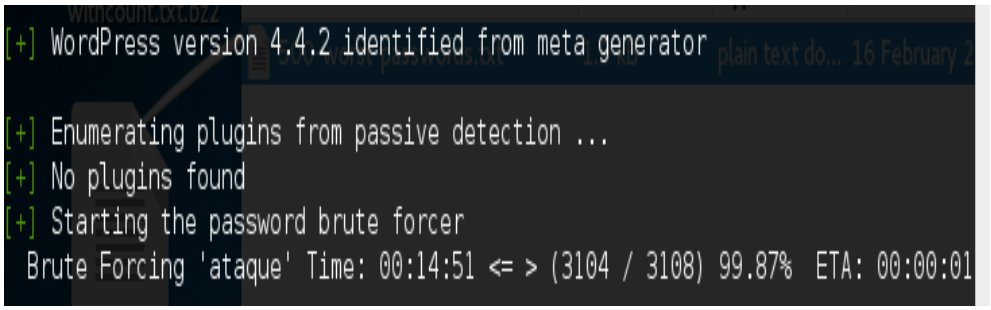

Fig. 13. Tiempo de respuesta de una ataque de fuerza bruta con WPScan.

Las estadísticas obtenidas en este trabajo de investigación permitieron diseñar un esquema efectivo de mitigación, que fue configurado mediante la formulación de reglas a nivel de Firewall Iptables en Linux Centos 6.7 más la instalación y configuración del Web Aplication Firewall Mod-security, asegurando la disponibilidad del servicio Web a los usuarios, tal como se muestra en las Fig. 14 y Fig. 15. La aplicación de este diseño de mitigación traerá beneficios inmediatos a los administradores y encargados de la red, debido a la facilidad del establecimiento de reglas a nivel de Firewall Iptables.

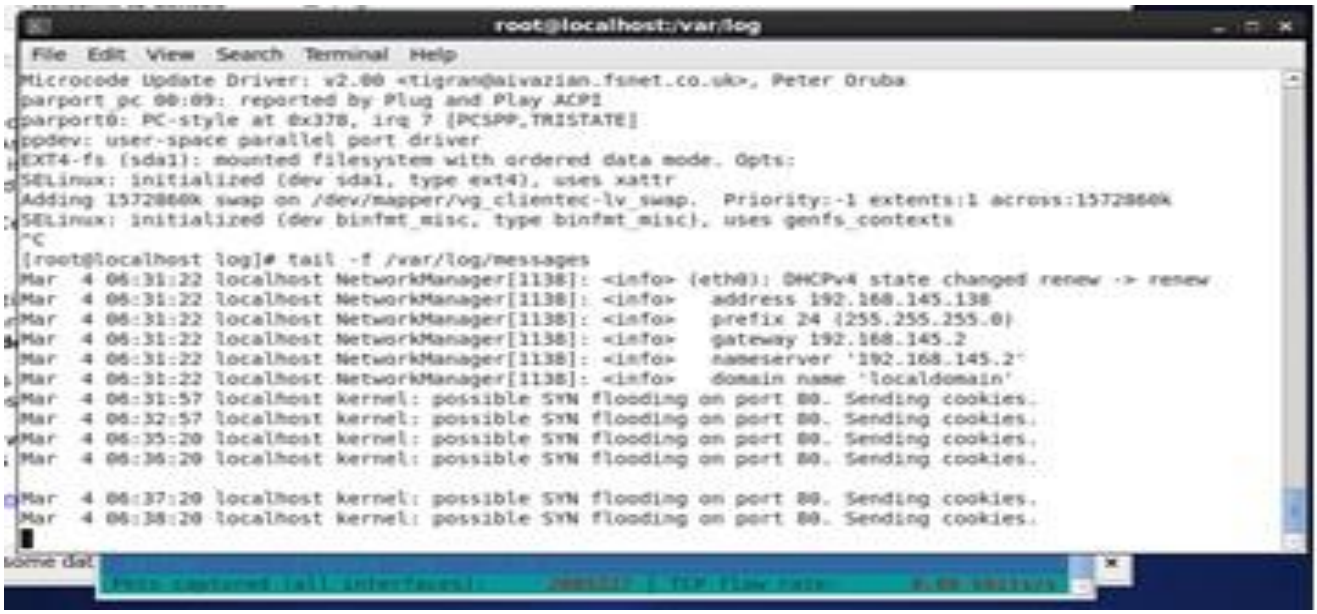

Fig. 14. Monitoreo de Mitigación de Ataque DDoS con WAF.

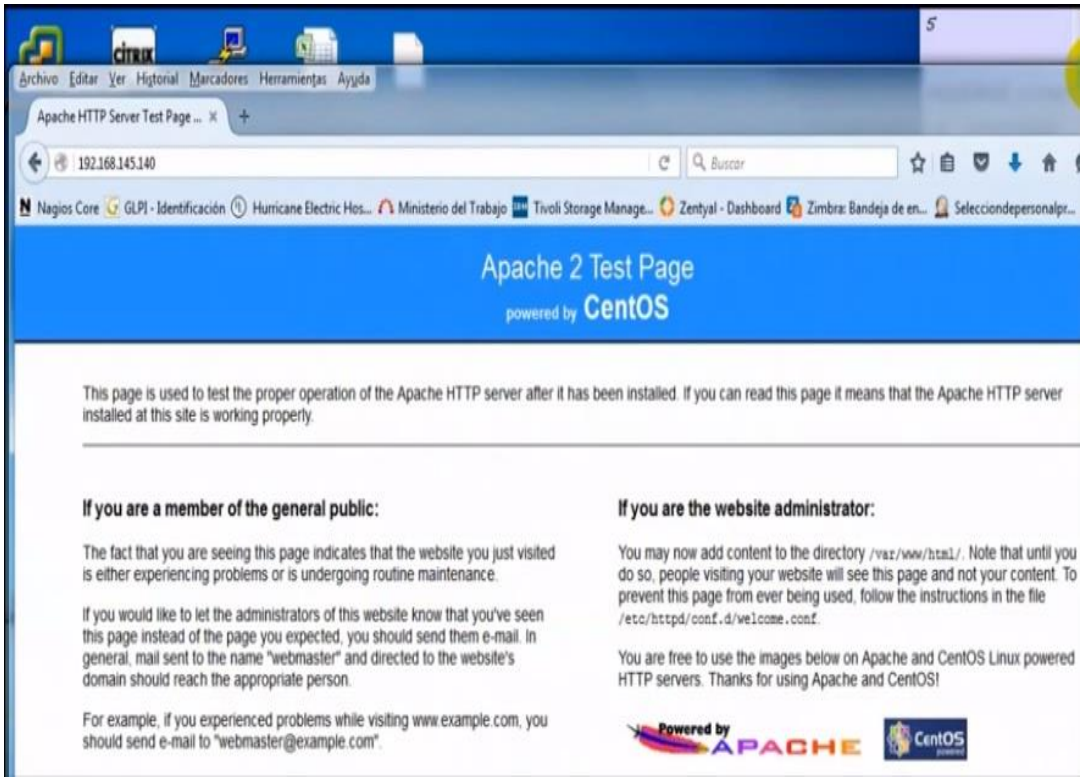

Fig. 15. Disponibilidad de Server Apache después de mitigación de ataque DDoS con WAF.

Trabajos relacionados.

Existen investigaciones que han implementado la virtualización de plataformas en el proceso de enseñanza-aprendizaje para realizar evaluación, análisis y mitigación de vulnerabilidades. Aquí se

incluyen algunas de las obras más relevantes encontradas y relacionadas con el trabajado realizado en esta investigación.

El trabajo en (Fuentes W, F. Rodas, and D. Toscano (2011) presenta un análisis de ataques UDP Flood mediante herramientas como UDP Unicorn, Longcat Flooder y UDPl.pl Script desarrollado en Perl, generando un mecanismo de detección y mitigación de los ataques a nivel del firewall e IDS/IPS. En la investigación realizada por Zapata et al. (2012) destaca la utilización de entornos virtuales para el desarrollo de prácticas de emulación para la realización de ataques, utilizando ataques de fuerza bruta se analizó las vulnerabilidades y se generó una solución en base a un demonio en Shell script que permitió detectar, controlar y mitigar dicho ataque. En (Mukhopadhyay, S. Goswami, and E. Mandal., 2014).

Los autores presentan una arquitectura para el análisis y obtención de vulnerabilidades mediante ataques realizados usando la herramienta Metasploit la misma que puede hackear éticamente un sitio. En el mismo contexto, en (Narváez Portillo, 2011). los autores trataron sobre la factibilidad de realizar unos Sistemas de Detección de Intrusiones mediante la implementación y configuración de la herramienta Kali Linux. Los autores destacan el uso de herramientas open source como el Mod-security como un firewall de aplicaciones web que (Méndez S. S. D. and D. O. R. López. 2013). funciona como un complemento que se instala en el servidor web. Actualmente soporta los servidores web Apache HTTPD, Microsoft IIS y NGinx. Provee protección contra las principales amenazas del Top 10 de OWASP 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.

CONCLUSIONES.

Este trabajo permite pasar de la teoría a la práctica y realizar un análisis y evaluación de herramientas que generan ataques DDoS de tipo SYN Flood y ataques de fuerza bruta a base de datos dentro de un ambiente virtualizado, se generaron ataques SYN Flood con la herramienta Metasploit y a base de datos en Mysql con la herramienta WPScan y para su detección y mitigación se desarrolló un mecanismo a través de la formulación de reglas eficientes a nivel de firewall Iptables en Linux Centos 6.7 más la instalación y configuración del Web Aplication Firewall Mod-security.

Desde el punto de vista estudiantil, existe un aprendizaje significativo al obtener conocimientos sobre la detección y mitigación de ataques de manera rápida y sin mayores costos, estos conocimientos adquiridos nos ayudaran en el campo profesional para evitar ataques en las empresas.

REFERENCIAS BIBLIOGRÁFICAS.

1. Fuentes W, F. Rodas, and D. Toscano (2011). Evaluación de ataques UDP Flood utilizando escenarios virtuales como plataforma experimental. Fac. Ing., vol. 20, No. 31, pp. 37–53.

2. Fuertes. W, J. E. L. de Vergara, and F. Meneses, (2009). Educational platform using virtualization technologies: Teaching-learning applications and research uses cases. Proc. II ACE Semin. Knowl. Constr. Online Collab. Communities, vol. 16. ISBN: 978-0-9842912-1-2.

3. Méndez S. S. D. and D. O. R. López. (2013). Firewall de Aplicación Web - Parte II, Seguridad. Def. Digit., pp. 1–3.

4. Mukhopadhyay, S. Goswami, and E. Mandal (2014). Web Penetration Testing using Nessus and Metasploit Tool. IOSR J. Comput. Eng., vol. 16, no. 3, pp. 126–129.

5. Narváez Portillo, (2011). Análisis de la Distribución Kali Linux, su Aplicación en la Configuración de uns Sistema Detector de Intrusiones y la Validación del Sistema en la Red de Datos de la Sede Sur de Quito de la Universidad Politécnica Salesiana. Tesis previa para la obtención del título de

Ingeniería en Electrónica. Universidad Politécnica Salesiana. Quito-Ecuador. https://dspace.ups.edu.ec/bitstream/123456789/10179/1/UPS%20-%20ST001825.pdf

6. OffSec Services Limited (2020). Metasploit Framework. Extraído el 13 de enero de 2020: https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
7. Ordoñez Pacheco L. D., (2009). La tecnología de la virtualización en las computadoras. CienciaUAT. No. 4, pp. 56–59, 2009.
8. The WPScan Team (2020). WPScan Package Description. Extraído de Kali Tools: https://tools.kali.org/web-applications/WPScan
9. Zapata Molina. (2012). Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución. Ingenius, No. 8, pp. 11–19

DATOS DE LOS AUTORES.

1. **Edgar Fabricio Rivera Osorio.** Máster en Gerencia de Sistemas. Docente de la Universidad Técnica Estatal de Quevedo, UTEQ-Ecuador. E-mail. eriverao@uteq.edu.ec
2. **Miriam Patricia Cárdenas Zea**. Magíster en Educación a Distancia y Abierta. Coordinadora de Maestría en Educación. Universidad Técnica Estatal de Quevedo, UTEQ-Ecuador. E-mail. mcardenas@uteq.edu.ec
3. **Washington Alberto Chiriboga Casanova**. Magíster en Sistemas de Información Gerencial. Decano de la Facultad de Ciencias de la Ingenieria, de la Universidad Técnica Estatal de Quevedo, UTEQ-Ecuador. E-mail. wchiriboga@uteq.edu.ec

RECIBIDO: 10 de marzo del 2020. **APROBADO:** 24 de marzo del 2020.