UNIVERSIDAD CATÓLICA DE CUENCA

SEDE AZOGUES

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE
LA INFORMACIÓN Y LA COMUNICACIÓN

TEMA:

ANÁLISIS DE DENEGACIÓN DE SERVICIOS EN SERVIDORES WEB WINDOWS Y LINUX.

TRABAJO DE TITULACIÓN
PRESENTADO EN CONFORMIDAD CON LOS REQUISITOS ESTABLECIDOS PARA LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS

Autor
EDISON GIOVANNY GONZÁLEZ GONZÁLEZ

Profesor Tutor
ING. MSC. Miguel Santiago Andrade López

Certificación Asesoría

Se certifica que:

El informe de investigación "Análisis de denegación de servicios en servidores WEB Windows y Linux.", de autoría del Señor Edison Giovanny González González CC: 0302302062, ecuatoriano, previo a la obtención del Título de Tercer Nivel corresponde Ingeniero de Sistemas, cumple con la caracterización, estructura y se sujeta a la normativa pertinente exigida por el Concejo de Educación Superior, CES y la Universidad Catoliza de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Azogues

Enero, 2020.

_____

Ing. Miguel Santiago Andrade López

Tutor

Certificación de Autoría

Certifico que:

"Análisis de denegación de servicios en servidores web Windows y Linux", es el tema de informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Tercer Nivel, por lo que, asumo su originalidad y el uso de fuentes de tercero registrados según las normas APA vigentes.

Azogues

Enero, 2020

_____

Sr. Edison Giovanny González González

CC: 0302302062

Agradecimiento

Educar es ser Modelo tanto en Responsabilidades como en Conocimientos,

Aprender es un proceso constante ya que la vida nunca nos dejara de enseñar,

Vivir es luchar por los sueños y deseos que se anhela en la vida,

Agradecer es saber reconocer el esfuerzo y dedicación de los demás, y una persona agradecida es bienvenida en cualquier lugar.

Agradecido con Dios, por todas sus bendiciones y todas las puertas que abrió en mi camino, Mi más sincero agradecimiento a todos y cada uno de mis profesores por su paciencia y perseverancia que han llevado durante este periodo de estudios, a mi Tutor por su guía en el desarrollo del presente trabajo de titulación.

A mis Padres por su constante apoyo y todas las oportunidades que me han otorgado, por compartirme sus enseñanzas y enseñarme una infinidad de valores a lo largo de mi vida logrando hacerme una persona de bien y enseñarme que cuando se quiere se puede y así conseguir todo lo que me eh propuesto.

Edison Giovanny González González

Dedicatoria

A mi Abuela Regina que me supo apoyar durante su vida aconsejarme hasta sus últimos días de su vida enseñarme que todo llega con sacrificio en la vida, a mis Padres por su apoyo incondicional ya que ellos fueron el pilar fundamental para que yo pueda concluir con esta meta más en mi vida con mucha admiración e infinito amor por el sacrificio les dedico mi trabajo de titulación.

Resumen

El presente trabajo tiene como objetivo principal el análisis y simulación de ataques (DoS) de Denegación de Servicios a Servidores Web Windows y Linux.

Para esto, se utilizó en Windows el sistema operativo Windows Server 2012 y para Linux Ubuntu Server 18.04.

La investigación abarca aspectos destacados sobre la aplicación de herramientas Open Source como son: Virtual BOX, Kali Linux para explotar las vulnerabilidades en los servidores tanto en Windows como Linux.

Se inició con una introducción a las redes de datos, servidores y servicios web, en el cual se revisan conceptos fundamentales de red, y todos aquellos aspectos involucrados en una red e internet y del trabajo en particular.

Posteriormente se presentó lo referente a ataques (DoS) de Denegación de Servicio. Además, y se realiza una breve revisión de los mismos y las herramientas para realizar el ataque.

Finalmente se mostró la parte Analítica y Explicativa, donde se simulo ataque de Denegación de Servicios (DoS) a los Servidores WEB, para comprender cómo se comporta un sistema atacado y como los Servicios se ven afectados, utilizando las herramientas antes indicadas, para brindar respuestas de como contrarrestar este tipo de ataque, con la recomendación de aplicativos, contrafuegos, parches los cuales evitarían la materialización de las amenazas detectadas.

Palabras Clave: Servidores, Redes, DoS, Ataques, Comunicaciones.

Abstract

The main objective of this research work is the analysis and simulation of a Denial-of-Service (DoS) attack on Windows and Linux Web Servers.

For this, the Windows Server 2012 operating system was used in Windows and for Linux Ubuntu Server 18.04.

The research covers highlights on the application of Open Source tools such as: Virtual BOX, Kali Linux to demonstrate vulnerabilities on servers in both Windows and Linux.

It started with an introduction to data networks, servers, and web services in which fundamental network concepts are reviewed and all those aspects involved in a network and internet and this paper in particular.

Subsequently, the Denial-of-Service (DoS) attacks were presented, and a brief review of them and the tools to perform the attack.

Finally, it was shown the analytical and explanatory section, where a Denial-of-Service (DoS) attack on WEB servers was simulated, to understand how an attacked system behaves and how the services are affected, using the tools mentioned, to provide responses on how to counteract this type of attack, with the recommendation of applications, firewalls, patches which would avoid the materialization of the threats detected.

Key words: Servers, Networks, DoS, Attacks, Communications.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Capítulo 1

1. Introducción

1.1. Antecedentes

En el presente trabajo de titulación, se realiza una revisión a los ataques informáticos, en específico a los de Denegación de Servicio (DoS) a Servidores Web sobre Windows y Linux a fin de precautelar los activos de información de la empresa, y en lo posible mitigar este tipo de amenazas y sus efectos negativos buscando soluciones para evitar esos tipos de ataques.

Garantizar la trasparencia, fiabilidad, beneficios y no rechazo de la información son los retos más grandes en la Seguridad de la información para un administrador de servidores web en las empresas. Uno de muchos procedimientos que emplean los hackers para cambiar la seguridad de una red es el Ataque de Denegación de Servicios.

Las redes de datos comparten mucha información por lo que son vulnerables a accesos no deseados. En este sentido, es imprescindible la localización de ataques de seguridad de los servicios que permitan una eficiente administración de la seguridad de la información.

En el 2013 se produjo un ataque DoS hacia los servidores del sistema de nombres de dominio de la organización Spamhaus la cual es una organización sin fines de lucro dedicada a ayudar a los proveedores de correo en la filtración de spam o correo no deseado. Este ataque provocó la ralentización del acceso a los servicios en Internet. El tráfico generado por los atacantes alcanzó los 300 Gigabits por segundo (Gbps) (Lee, 2013).

Otro ataque DoS más reciente es el que sufrieron los servidores de la empresa DigitalOcean, proveedor estadounidense de servidores virtuales privados. El ataque fue

realizado el 24 de marzo de 2016 y este provocó que los servidores no puedan responder las consultas Domain Name System o también conocido como DNS debido a un incremento excesivo de las consultas a registros de un dominio (PTR) (DigitalOcean, 2016).

En la actualidad, por medio de las redes informáticas, se comparte un alto volumen de información, que por lo general están disponibles para la mayoría de personas con acceso a internet, por lo tanto, es necesario analizar este tipo de riesgos que día a día se han incrementado, a fin de evitar falencias de seguridad de los servicios y que permitan una eficiente administración.

1.2. Descripción del problema

La Seguridad de la información en el mundo actual es indispensable y sus aplicaciones están prácticamente en todas las actividades que realiza el ser humano, permitiendo la agilidad de procesos que manualmente llevaría mucho más tiempo si no fuera por la ayuda de la tecnología, cambiando la manera de trabajar, comunicarse, realizar trámites, e inclusive la forma en que operan los delincuentes.

Pero a través de la seguridad de la información nació un valor especial de esta información por el cual se crearon diferentes métodos hasta la actualidad y se sigue creando nuevos métodos para poder vulnerar esta información, ya sea para ser hurtada, modificada, para beneficio de terceros.

Siempre que la información es privada tiene más valor para un atacante por el hecho de mientras más privada sea la información más valor generara al atacante de lograr accederla, por eso es que se ha creado un sin número de herramientas y métodos para poder vulnerar la seguridades de la información una de ellas es el ataque de Denegación de Servicios también conocida como DoS (Denial of Services) que tiene por objetivo

atacar un grupo o una red de computadores causando que sus servicios sean inaccesibles para los usuarios.

En los últimos años la transformación, y la posterior novedad de la tecnología ha producido avances en todo el entorno a nivel mundial, es así que la intranet y el internet son medios indispensables para el cambio de información, la gran cantidad de establecimientos públicos y privados emplean estos medios para hacer actividades como por ejemplo: envío de correo electrónico, transacciones bancarias, declaración de impuestos, intercambio de información, es decir, con el desarrollo tecnológico aumentado los métodos de vulnerabilidades y ataques informáticos que usan los hacker, "Persona que se dedica a acceder ilegalmente a los sistemas informáticos, y usan su conocimiento para demostrar una vulnerabilidad y corregirlo" (Significados, 2018), o crackers, "Personas que se dedican encontrar vulnerabilidades en los sistemas informáticos y los modifican o perjudican para obtener beneficios" (Significados, 2018), para realizar intrusiones e infiltraciones a una determinada red como ya se menciona anteriormente uno se ellos.

Como ya se mencionó anteriormente el atacante que utilice DoS genera problema al causar que los servicios sean inaccesibles por usuarios genera un gran daño tanto al proveedor de servicios como el usuario generando grandes inconvenientes, riesgos, pérdidas monetarias, transacciones en ambas partes.

En el presente trabajo de investigación se demostrará un ataque de Denegación de servicios DoS específicamente a servidores web mediante herramienta que permita que los servidores queden sin acceso a los servicios provocando que la accesibilidad sea nula hacia los servicios de los servidores web.

El riesgo es cada vez más peligroso ya que las organizaciones se manejan en la actualidad la mayor parte de su información mediante la web por lo que es víctima de cualquier ataque de Denegación de servicios a sus servidores DoS ya que tanto las empresas públicas y privadas que generan pequeño, medio o gran valor están en la lista de ciberdelincuentes que están día a día actualizándose como vulnerar las seguridades que implementa cada empresa u organización.

Hay una variedad de ataques de Denegación de servicios a nivel básico como para hacer que un recurso de una red quede inutilizable, ataques de flujo por nivel de aplicación que pueden crear múltiples formas para enviar grandes cantidades de peticiones a servidores web deseados, ataques crash estos mandan paquetes de forma que se aprovechan de algún error de los sistemas operativos generados mediante exploits.

La comunicación es un elemento indispensable para el hombre, las redes proveen un canal de comunicación eficiente, donde se comparte información cada vez más sensible o de carácter más personal, por ello, es necesario encontrar herramientas que brinden protección contra riesgos como robo o suplantación de la identidad de los usuarios, la información privada puede ser violada, los cortafuegos pueden ser corrompidos, las medidas de seguridad violadas o las redes saboteadas mediante herramientas como la de Denegación de servicios DoS.

La utilización de Denegación de servicios es utilizada mucho por cibercriminales porque es mucho más barato, difícil de detectar y altamente efectivo. Los ataques de DoS son difíciles de detectar ya que a menudo utilizan conexiones por defecto e imitan un tráfico autorizado normal, y es altamente efectivo porque los servidores objetivos confían por error en el tráfico y por lo tanto facilitan el ataque ejecutando alguna petición del atacante.

La necesidad de intercambiar información es de vital importancia, así como el de protegerla.

Para la protección de estos datos, se deben establecer mecanismos que validen la información que se puede recibir y transmitir. Analizando las soluciones existentes, se encuentra que es viable la creación de un proceso de seguridad, el cual, tendrá como base el grado de certeza obtenido durante la fase de clasificación del flujo de datos de la red, logrando una correcta distinción de un flujo representativo de ataque y de un flujo normal. Diariamente son generados miles de datos y almacenados en dispositivos físicos o virtuales, haciendo de estos elementos tecnológicos los escenarios perfectos para personas que lucran de la información obtenida ilegalmente. Dado que la información es un activo muy importante y que merece extrema precaución, pues la pérdida o divulgación de esta información puede causar pérdidas económicas, de imagen y afecta a la productividad de las empresas o personas (Serra Ruiz J, 2009).

1.3. Formulación del problema

¿Se puede controlar los ataques de denegación de servicios a servidores WEB?

1.4.Descripción Metodológica

La metodología a utilizar en el presente trabajo de titulación será la investigación Aplicada, el cual será aplicada para analizar el comportamiento de Denegación de servicios (DoS) en Servidores Web tanto en Linux como Windows, en los cuales se determinará las vulnerabilidades existentes y posteriormente contrarrestar las mismas.

Se trata de un tipo de investigación centrada en encontrar mecanismos o estrategias que permitan lograr los objetivos propuestos. Por consiguiente, el tipo de ámbito al que se aplica es muy específico y bien delimitado, ya que no se trata de explicar una amplia variedad de situaciones, sino que más bien se intenta abordar un problema específico planteado. (Rodriguez, 2019)

- En este tipo de investigación el problema está establecido y es conocido por lo que utiliza para dar respuestas a los problemas en específico. (Rodriguez, 2019)
- En este tipo de investigación el énfasis del estudio está en la resolución práctica de problemas. (Rodriguez, 2019)

1.5. Objetivos

1.5.1. Objetivo General

Simular y analizar el ataque de Denegación de servicios (DoS) utilizando herramientas open source sobre servidores web, determinar las vulnerabilidades existentes y obtener un resultado en el cual ayude a contrarrestar estos ataques.

1.5.2. Objetivos Específicos

- Determinar y analizar los diferentes ataques de denegación de servicios.
- Simular servidores Web realizando ataques de Denegación de servicios (DoS), complementarlo con las leyes vigentes en el Ecuador (COIP) por medio de políticas de firewall.
- Determinar los riesgos y vulnerabilidades que sean encontrados en este estudio y analizar las posibles soluciones ante las amenazas a presentarse.

1.6. Contribución

Una sólida propuesta que minimice los efectos del ataque de Denegación de Servicios (DoS) de manera puntual, dejando a un lado los tratamientos tradicionales a este problema, pues ninguna de estas soluciones da un tratamiento efectivo a los efectos de dicho ataque. El análisis propuesto, es relativamente manejable y además económico, así cualquier estudiante o futuras generaciones pueden ampliar y utilizar este estudio.

Con esto se pretende reducir las pérdidas económicas y otras que pudieran generarse debido a los efectos del ataque de Denegación de servicios (DoS).

1.7. Estado del arte

- **El Caso Ronnie España (Ataque DoS: Denegación de Servicio)**

El ataque iniciado entre los días 24 y 25 de diciembre de 2002, repitiéndose cada 2 días, a veces con cuatro y cinco ataques diarios, hasta mayo de 2003, entre abril y mayo, arremetió también contra los proveedores que dan soporte a la red de chats de IRC-Hispano.

El autor del ataque fue Santiago Garrido o también conocido como “Ronnei” de 26 años, utilizo el seudónimo ‘ronnei’ a su ataque, El objetivo fue “IRC-Hispano”, la mayor red de habla hispana con 16 millones de usuarios al mes, fue una de las organizaciones más afectadas por este ataque, y posteriormente ataco también Wanadoo, Ono y LleidaNet.

La motivación del ataque ronnie fue por venganza según la guardia civil, al haber sido expulsado del chat IRC-Hispano por conectarse a ella “a través de un ordenador V-host, que tenía como fin dificultar su identificación”, una conducta ilícita en IRC-Hispano. (Acaparros, 2016)

El ataque que utilizó fue un gusano denominado “deloder” para infectar ordenadores vulnerables de Europa y Asia, convirtiéndolos en “zombies” desde donde realizó el ataque DoS y DDoS (Ataque de Denegación de servicios Distribuido), sobrecargando las redes con un bombardeo con paquetes de datos hasta que consiguen dejarlas inoperativas. Una sola maquina cliente difícilmente podría desbordar un servidor, pero si al coordinar agresiones desde varias máquinas clientes hacia un mismo servidor, al desbordar su capacidad de respuesta. (Acaparros, 2016)

Dimensión o amplitud del ataque: Llegó a afectar en algunos momentos al 30% de los internautas españoles, unos 3 millones de usuarios según la Unidad de Delitos Telemáticos de la Guardia Civil LA PRIMERA SENTENCIA POR ATAQUE DE DENEGACIÓN DE SERVICIO EN ESPAÑA La Unidad de Delitos Telemáticos de la Guardia Civil, inició una operación que contó con la colaboración de la empresa antivirus Panda Software y que concluyó con la detención de ‘Ronnie’ en agosto de 2003, El 7 Febrero de 2006, ha sido condenado a dos años de prisión por delitos de daños continuados, valorados en 1.332.500 euros de responsabilidad civil, desglosados en: 474.500 € en daños a LLEIDA.NET 570.716 € en daños a WANADOO,120.000 € en daños a ONO, 218.000 € en daños a IRC-HISPANO, además deberá pagar 18 meses de multa con una cuota diaria de 6€.

Técnica utilizada para el ataque. ¿Qué es un ataque DoS? ataque de Denegación de Servicio. La detección de un ataque DoS mediante NIDS (Network Intrusión Detección Systems) es más complicada, puesto que es difícil saber el origen real del atacante.

Descripción del ataque: Ataques DoS Utilizar los ataques para tomar el control de N máquinas y provocar de esta manera un ataque coordinado contra una tercera máquina. Ronnie utilizo el gusano "es un programa de software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores sin que te des cuenta de que el equipo está infectado." como programa instalado en la máquina víctima, que delegan el control de la misma al atacante, permitiendo el acceso remoto. Infectando ordenadores vulnerables de Europa y Asia, convirtiéndolos en "zombies" (SophosLabs estima que más del 60% del spam originado hoy en día proviene de ordenadores zombis). UPC 5 Denegación de servicio † La denegación de servicio DoS (Denial of Service), se produce cuando un determinado servicio no se encuentra disponible. En este caso se provocó que no hubiese ancho de banda suficiente, y que no hubiese recursos en el sistema. (Acaparros, 2016)

La ejecución del ataque DoS se convino con un ataque DDoS para que sea un ataque masivo contra los nodos centrales de IRC Hispano mediante paquetes ICMP (ping). Ronnie agoto el ancho de banda del IRC, envío paquetes ICMP echo request de forma continuada de tamaño grande (ping), IRC respondió con ICMP echo reply (pong)

Medidas de prevención sé que tomaron en el ataque ronnie: Para prevenir este tipo de ataque, tener el sistema operativo siempre actualizado, tener un buen el nivel de seguridad como passwords seguras, instalando firewalls, desinstalando servicios sin utilizar, y filtrando paquetes, que impidan IP spoofing, Además de planificar la detección, mitigación y el uso de empresas especializadas, servicios y herramientas disponibles para ello. Para evitar que se repita el ataque en la empresa y acaben siendo utilizadas para este tipo de ataques, se implementó herramientas como las que ofrece INCIBE en su Servicio

Antibotnet o particulares OSI ofrece su Servicio Antibotnet para PC,s y móviles. (Acaparros, 2016)

- **Ataque plataforma GitHub en el año 2018 en los Estados Unidos**

GitHub y un segundo sitio web cuyo nombre no fue develado, fueron los afectados por los ataques DoS más grandes que se registraron hasta el momento.

Con tan solo cuatro días de diferencia, se registraron los dos ataques "de denegación de servicio" (DoS, por sus siglas en inglés) más grandes de los que se haya tenido registro hasta el momento. El primero de ellos ocurrió el miércoles 28 de febrero, cuando GitHub quedó fuera de servicio desde las 17:21 a las 17:26 (UTC) y fuera de servicio, pero de manera intermitente, desde las 17.26 a las 17:30 horas, explicó la empresa en una publicación realizada en su página web.

El segundo fue el pasado lunes 4 de marzo de 2018, cuando la empresa de seguridad y monitoreo Arbor Networks afirmara que su sistema de datos de amenazas DoS y DDoS tráfico global, llamado ATLAS, registró un nuevo ataque de esta naturaleza contra el sitio web de sus clientes, cuyo nombre no fue develado, en Estados Unidos.

En su pico máximo, el ataque a GitHub alcanzó un tráfico entrante de 1.35 terabits por segundo (Tbps), superando el anterior record de 1 Tbps al que había llegado el ataque al proveedor de servicios de hosting francés OVH, en septiembre de 2016. Por su parte, el segundo de los ataques registró un pico de tráfico de 1.7 Tbps, convirtiéndose de esta manera en el máximo registrado hasta el momento. (Gonzalez, 2018)

Memcrashed

A diferencia del ataque contra OVH, donde el bombardeo de tráfico fue desatado por dispositivos de Internet de las Cosas (IoT) controlados por la botnet Mirai, en ninguno de estos dos recientes ataques hubo aprovechamiento de algún dispositivo comprometido.

En los dos casos registrados, los atacantes incorporaron la ampliamente utilizada base de datos de los servidores Memcashed para evitar estos ataques; que soportan el protocolo UDP habilitado y que se ofrecen en Internet sin ningún requerimiento de autenticación en el lugar, utilizando un método de ataque relativamente poco común apodado "Memcrashed" que es un nuevo método de ataque, un ataque brutal aprovechando el puerto 11211 de Memcached al cual se le conoce con el nombre de Memcrashed. Peligroso donde los haya nos puede generar en segundos más de un terabyte de tráfico. "Memcached" es un sistema de alto rendimiento de caché de objetos opensource. Aunque sus posibilidades son grandes, se suele utilizar para almacenar en caché los datos de sesión del servidor web de manera que se acelera considerablemente la navegación por el sitio, y ahí es donde comienza el problema. (Gonzalez, 2018)

Los servidores están diseñados para aumentar la velocidad de sitios y aplicaciones web, aunque también pueden ser utilizados como reflectores para amplificar el tráfico hacia un servicio específico. De hecho, según el servicio de protección de DoS Cloudflarela, la respuesta puede llegar a ser 51,200 veces mayor que la solicitud.

En el caso de GitHub, el atentado implicó engañar la dirección IP de los servicios y enviar pequeñas y repetidas solicitudes a un número de servidores; los cuales respondieron debidamente, excepto por el hecho de que provocaron respuestas inmensamente desproporcionadas.

“Ocultar la dirección IP permite direccionar la respuesta de los servidores memcached hacia otra dirección, como la que utiliza GitHub.com, y enviar más datos de los necesarios hacia el destinatario por parte de la fuente original”, explicó la compañía GitHub mediante un post. (Gonzalez, 2018)

Las medidas de prevención después que el ataque DoS comenzara, GitHub se suscribió a la ayuda que ofrece el servicio de Akamai Prolexicu, expertos en mitigación de ataques DoS; quienes redujeron el tráfico basura redirigiéndolo a través de su red y bloqueando las solicitudes maliciosas. Finalmente, el atentado cesó. (Gonzalez, 2018)

Capítulo 2

2. Marco Teórico

2.1. Pasos a cumplir en la Investigación Aplicada.

Como antes ya se mencionó en la descripción metodológica que se utilizó la metodología aplicada en el presente trabajo existen ciertos pasos que se deben cumplir los cuales están a continuación:

a) La investigación aplicada depende de la investigación básica. Esto es porque se basa en sus resultados.

b) La investigación básica es la investigación pura, basada en un marco teórico.

c) Así mismo, la investigación aplicada requiere obligatoriamente de un marco teórico, sobre el cual se basará para generar una solución al problema específico que se quiera resolver.

d) Por otro lado, la investigación aplicada se centra en el análisis riesgos y solución a los problemas.

e) Además, se nutre de los avances y se caracteriza por su interés en la aplicación de los conocimientos.

Fases de la investigación Aplicada.

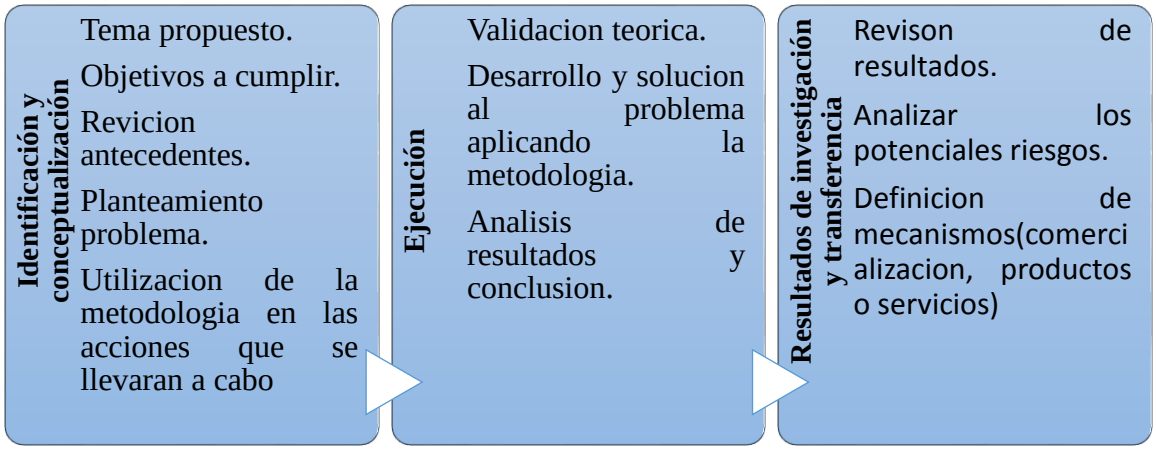

Figura 1: Solución Metodológica Aplicada.
Fuente: (Rodriguez, 2019)

Continuando con la metodología aplicada se procede a cumplir cada uno de los pasos y fases que debe cumplir la misma.

2.2. Hacking

"Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño" (Tori, 2008a).

Hacking, es una palabra que, presentada en un contexto global es un conjunto de maniobras que se interpretan como piratear y romper la seguridad de un sistema de forma ilegal, además que la palabra hacker es traducida generalmente como pirata o delincuente informático. (Cruz Saavedra, 2014)

Si a "Hacking" se le añade la palabra "Ético", se puede definir como los profesionales de la seguridad informática que utilizan sus conocimientos de hacking con fines defensivos para demostrar al usuario o potencial victima las vulnerabilidades encontradas en su red o sistema informático donde el activo más valioso es la información que circula y almacena en éste, para luego de realizadas las pruebas proponer las recomendaciones correspondientes que proporcionen un nivel de seguridad aceptable para la red y se puedan mitigar los riesgos de ataques. (Leandres, 2019)

2.3. Modos de hacking

"La infraestructura informática de una organización o empresa puede ser probada y analizada de varias maneras" (Gaibor, 2007a).

Los modos más comunes de hacking ético son:

- Ataque local.
- Ataques con equipo robado.
- Ataques a entradas físicas de la organización.
- Ataques por medio de equipos sin autenticación.

2.4. Ataque local

Es la simulación de un ataque desde el interior de la red u organización, el cual, puede ser un empleado o un hacker que ha obtenido privilegios legítimos para acceder al sistema y equipos de la red; su implementación puede tornarse sencillas debido al gran número de herramientas que se encuentran en la Internet. (Gaibor, 2007b)

2.4.1. Ataques con equipos robados

En el mundo real, a menudo computadoras portátiles son sustraídas, con el objetivo de evaluar cómo los usuarios protegen la información. Por ejemplo, si una computadora portátil robada tiene almacenadas contraseñas o información crítica que puede ser de fácil acceso, esto puede ser una vulnerabilidad para la organización. Los atacantes podrían conectarse remotamente (vía DialUp o VPN) a los equipos de la empresa con autenticaciones verdaderas. (Gaibor, 2007c)

2.4.2. Ataques a entradas físicas de la organización

Con estas pruebas se busca probar los controles físicos de la organización, tales como puertas, salidas, seguridades, circuito cerrado de televisión (CCTV).

Para lograr este fin, el atacante deberá intentar ingresar al edificio de la organización; las defensas primarias en este caso es una política de seguridad bien implementada, guardias de seguridad, controles de acceso, monitoreo y por supuesto, conocimiento de la seguridad. (Sanchez J. A., 2013a)

2.4.3. Ataques por medio de equipos sin autenticación

Esta prueba está identificada para buscar puntos de acceso Inalámbricos o módems; se trata de ver si los sistemas son lo suficientemente seguros y tienen activados los debidos controles para autenticación necesarios.

Si estos controles pueden ser pasados por alto, el hacker ético puede comprobar hasta qué nivel de control puede obtener con ese acceso. (Saltos, 2017a)

2.5. Ataques a redes informáticas

Es una invasión a la seguridad del sistema que se deriva de una maniobra bien planeada y actualmente, sus técnicas de ataques son cada vez más sofisticadas, ya que son más difíciles de prevenir y su capacidad de hacer daño son ilimitadas, debido a que atacan vulnerabilidades de diseño, operación y configuración de la red. (Saltos, 2017b)

2.5.1. Ataque de escaneo de puertos

"El escaneo de puertos es una técnica que se basa en la evaluación de vulnerabilidades por parte de hackers o administradores para auditar las máquinas y la red" (Osabuena, 2015a).

Existen aplicaciones que permiten verificar la seguridad de un computador en una red, a través del análisis de sus puertos, localizando los puertos abiertos o cerrados, los servicios que están ofrecidos, identificar si esta implementado un Firewall con el fin de tomar control remoto del pc víctima. (Osabuena, 2015b)

2.5.2. Tipos de escaneo de puertos

Los tipos de escaneo de puertos son:

- **TCP Connect**

  Es una técnica común que no necesita de ningún tipo de privilegio especial y que se puede ejecutar a través de un software de escaneo de puertos. Consiste en usar la llamada connect () de TCP para intentar establecer una conexión con cada uno de los puertos del equipo a escanear. Si la conexión se establece, el puerto está abierto; si el puerto está cerrado, se recibe un aviso de cierre de conexión y, en caso de no recibir respuesta, el puerto se encuentra silencioso. (Gutierrez, 2013a)

- **TCP SYN**

  También conocido como escaneo medio abierto, es una técnica que intenta establecer conexión mediante el envío de un flag SYN, si existe una respuesta del Host con el paquete SYN+ACK, la conexión se interrumpirá al enviar el paquete RSP, evitando quedar registrado por parte del sistema. (Gutierrez, 2013b)

- **TCP FIN**

  Conocido como escaneo silencioso, consiste en enviar un paquete FIN al host de destino, los estándares de TCP/IP indican que al recibir un paquete FIN en un puerto cerrado, se responde con un paquete RST. Si se recibe un paquete RST por respuesta, el puerto está cerrado, y en caso de no recibir respuesta (se ignora el paquete FIN) el puerto puede encontrarse abierto o silencioso. Este tipo de escaneo no tiene resultados fiables. (Gutierrez, 2013c)

- **ACK Scan**

  Permite identificar de manera confiable, si un puerto se encuentra en estado silencioso. Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia y confirmación aleatorios. Cuando reciba el paquete, si el puerto se encuentra abierto, responderá con un paquete RST, pues no identificará la conexión como suya; si el puerto está cerrado responderá con un paquete RST, pero si no se obtiene respuesta podemos identificar claramente el puerto como filtrado (puerto silencioso). (Gutierrez, 2013d)

2.6. Ataque de denegación de servicio (DoS)

El ataque de denegación de servicio tiene como objetivo dejar inaccesible a un determinado recurso de un servidor. Estos ataques generalmente se llevan a cabo mediante el uso de herramientas que envían una gran cantidad de paquetes de forma automática para desbordar los recursos del servidor logrando de esta manera que el propio servicio quede inoperable. Además, se suelen coordinar ataques involucrando un gran número de personas para que inicien este tipo de ataque simultáneamente, tratándose así de un ataque de denegación de servicio distribuido. (Catoira, 2012)

Los ataques de Denegación de Servicio son los siguientes:

- **Ataque lógico o software**

  Consiste en enviar al equipo remoto una serie de datagramas mal construidos para aprovechar algún error conocido en dicho sistema. Los tipos de ataques lógicos son Ping de la muerte, Teardrop y Land. (Saltos, 2017b)

- **Ataque de inundación (flood)**

  Consisten en bombardear un sistema con un flujo continuo de tráfico que intenta consumir todos los recursos y el Ancho de Banda de la red del sistema atacado. Los tipos de ataques de inundación más comunes son TCP SYN, Smurf IP, UDP Flood e ICMP Flood. (Saltos, 2017c)

- **Ataque de fuerza bruta**

  Es una técnica que proviene originalmente de la criptografía, en especial del criptoanálisis (el arte de romper códigos cifrados o descifrar textos). Es una manera de resolver problemas mediante un algoritmo simple de programación, que se encarga de generar y de ir probando las diferentes posibilidades hasta dar con el resultado esperado o de mejor conveniencia. (Tori, 2008b)

  Las técnicas de fuerza bruta son:

  - Uso de diccionarios
  - Paralelización en Clusters
  - Clusters con botnets
  - Paralelización con GPUs.

- **Ataque de hombre en el medio**

  Consisten en realizar una técnica de ataque pasivo, denominada: ARP Spoofing, y se lleva a cabo en redes LAN y WLAN. Al estar conectados en la misma red, este ataque permite capturar todo el tráfico dirigido de uno o varios hosts de la red a la puerta de enlace configurada (Gateway) y viceversa, para engañar o envenenar la caché de la tabla ARP de la víctima. (Lois, 2012a)

  De modo, que la dirección MAC Address (Media Access Control Address) de la puerta de enlace de la víctima no sea la verdadera, si no que sea la dirección

> MAC del atacante. Así cuando la víctima realice consultas hacía Internet que serán requests para su gateway antes pasaran por el host del atacante, este lo dejará pasar al router y devolverá la respuesta al atacante de nuevo y este a la víctima. De esta manera que la víctima no se dará cuenta de lo que está sucediendo. (Lois, 2012b)

2.7.Redes informáticas

"Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí, por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos, directorios e impresoras" (Velez, 2006).

"Para crear la red es necesario un hardware que una los dispositivos (tarjetas, cables) y un software que implemente las reglas de comunicación entre ellos (protocolos y servicios)" (Bueno, 2012).

La instalación de una red, supone la unión de todos aquellos elementos que antes trabajaban de manera separada. De esta forma se crea un sistema de comunicación que elimina los problemas de distancia y facilitan la compartición de los elementos disponibles en los ordenadores y servidores dentro de una red informática. (Sanchez J. A., 2013b)

2.8.Virtualización

Es una técnica empleada que implica generar que un recurso físico como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fueran varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico. (Velazquez, 2009)

“La virtualización crea una nueva plataforma informática conformada por los recursos virtuales que comunica las aplicaciones del negocio y las plataformas informáticas físicas originales” (Ulloa, 2009).

2.8.1. Tipos de virtualización

Existen dos tipos de virtualización:

- **Virtualización completa.** También llamada nativa. La capa de virtualización, media entre los sistemas invitados y el anfitrión, la cual incluye código que emula el hardware subyacente para las máquinas virtuales, por lo que es posible ejecutar cualquier sistema operativo sin modificar, siempre que soporte el hardware subyacente. El código de emulación puede provocar pérdida en el rendimiento. (Fernandez, 2010a)
- **Paravirtualización.** Similar a la virtualización completa porque introduce hipervisor como capa de virtualización, pero además de no incluir emulación del hardware, introduce modificaciones en los sistemas operativos invitados que por consiguiente están al tanto del proceso (deben poder ser modificables). (Fernandez, 2010b)

2.8.2. Herramienta de virtualización VirtualBox

Este software es uno de los más utilizados cuando se comienza en el mundo de la virtualización, inicialmente desarrollado para arquitecturas de x86 la empresa alemana que lo desarrolló se llama Innotek, que también contribuyó al desarrollo de OS/2 y el apoyo en la virtualización de Linux y versiones de OS/2 de productos pertenecientes a connectix que posteriormente fueron adquiridos por Microsoft. VirtualBox está más enfocado a virtualización de escritorios remotos, con relación a otros sistemas de mayor

rendimiento como Citrix, o VMware, en febrero de 2008 la empresa Innotek pasó a ser propiedad de Sun Microsystems (Mejia, 2018a).

VirtualBox tiene una licencia que es un paquete completo que está destinado hacía un uso de ¨proprietary Personal Use and Evaluation License" (PUEL), que es una licencia gratuita, educativo. Licencias de uso comercial de esta versión de VirtualBox se pueden comprar en Sun. Una segunda versión llamada VirtualBox Open Source Edition (OSE) es una versión libre publicada bajo la "GNU General Public License" (GLP), (ecured, s.f.) (Mejia, 2018b).

2.9. Servidores

"Un servidor, es un equipo informático que está al servicio de otro host, personas llamadas clientes y que les abastecen a éstos, todo tipo de información. Entre los equipos clientes pueden ser personas u otros dispositivos móviles, impresoras" (Garcia, 2006).

2.9.1. Servidor web

Es un programa que implementa el protocolo HTTP (Hypertext Tranfer Protocol). Este protocolo pertenece a la capa de aplicación del modelo de interconexión de sistemas abiertos (OSI) y está diseñado para transferir hipertextos, páginas web y paginas HTML (Hypertext Markup Language); generalmente funciona a través del puerto 80. (Romero, 2014)

2.9.2. Servidor web Apache

Es el servidor más utilizado, aunque ha vivido tiempos mejores. Parte de su éxito se debe a que es multiplataforma y a su estructura modular, que permite emplear diversos lenguajes en el lado del servidor (PHP, Python y Perl principalmente), así como incorporar características como la compresión de datos, las conexiones seguras y la utilización de URLs amigables. (Bruno Chavarria Neira, 2017)

2.10. Administración de redes

Es un conjunto de técnicas que permite mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. Los principales objetivos de la Administración de redes son:

- Mejorar la continuidad en las operaciones de la red con mecanismos adecuados de control y monitoreo para la resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar de mejor manera los recursos, entre ellos el ancho de banda, impresoras, etc.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios (Aguilar, 2007).

2.10.1. Herramientas de administración y monitoreo de redes

"Las herramientas de seguridad y monitoreo de redes se dividen en gestión de usuarios, gestión del hardware, gestión del software y monitorización de la actividad de red y seguridad" (Sanchez J. A., 2013c).

2.10.2. Monitoreo de la actividad de red y seguridad

El monitoreo de la red es indispensable para poder detectar todo tipo de errores y eventos que puedan influir en la performance de la misma, para esto se tienen muchas

herramientas que pueden analizar los diferentes niveles de las capas de red. (Sanchez J. A., 2013d)

2.10.3. Aplicaciones para el monitoreo de red y seguridad

2.10.3.1. Wireshark

"Antes conocido como Ethereal, permite analizar los protocolos utilizados en la red para solucionar problemas de comunicación. Es una herramienta multiplataforma y gratuita" (Alvarez, 2013a).

Las características de Wireshark son: a.-Disponible para Linux y Windows, b.-Captura de paquetes en vivo desde una interfaz de red, c.-Muestra los paquetes con información detallada de los mismos, d.-Abre y guarda paquetes capturados, e.-Importar y exportar paquetes en diferentes formatos, f.-Filtrado de información de paquetes, g.-Resaltado de paquetes dependiendo el filtro, h.-Crear estadísticas. (Alvarez, 2013b)

2.10.3.2. Webmin

Es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix. Con él se pueden configurar aspecto interno de varios sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc. (Desdelinux, s.f.)

- Puede configurar cuentas de usuarios, Administración de servicios como Apache, DNS, Squid, compartición de archivos, entre otros. (Sanchez J. A, 2013e)

2.11. Kali Linux

Kali es una distribución de Linux basada en Debian. Su objetivo es simple; incluya tantas herramientas de penetración y auditoría de seguridad como sea posible en un

paquete conveniente. Kali entrega también muchas de las mejores herramientas de código abierto para realizar pruebas de seguridad que se recopilan y están listas para usar. (Masgnulinux., 2018)

Kali es desarrollado y mantenido por Offensive Security. Son una presencia conocida y confiable en el mundo de la seguridad, e incluso certifican a los profesionales de la seguridad con algunas de las certificaciones más respetadas disponibles. (Masgnulinux., 2018)

Permite a sus usuarios tomar ventaja de la herramienta Advanced Package (APTO) que proporciona expertos con la posibilidad de añadir varios repositorios de terceros. Permiten a los administradores establecer sus propios anfitriones, espejos y puertas de enlace y de gestionar las instalaciones de software. (Sensors tech forum, 2017)

2.12. Metasploit

Es como una infraestructura que se puede utilizar para construir herramientas de "hacking a medida". O a su vez se denomina conjunto de herramientas de explotación, Metasploit permite ser ejecutado de diferentes formas, desde línea de comandos, en donde se aceptan cada uno de los comandos Metasploit de forma independiente, por interfaz web (deprecada en las últimas versiones y disponible únicamente en versiones antiguas), o por medio de la consola unificada de Metasploit llamada msfconsole (se trata de un intérprete de comandos bastante robusto que es el sustituto de la interfaz web), esta última es la más utilizada por aquellos que utilizan Metasploit para realizar sus pruebas de penetración. (Posada, 2013)

2.12.1. Comandos básicos de Metasploit

Entre sus variantes de funcionamiento, aquí detallo los comandos básicos para su modo consola. (MetaSploit, 2011)

- help: Tal como su nombre indica permite obtener ayuda en un contexto determinado (exploit o module).

- back: Permite salir del contexto actual de ejecución (exploit o module)

- check: Aunque no todos los exploits lo soportan, permite ver si un objetivo determinado es vulnerable al exploit que se encuentra actualmente seleccionado en la consola.

- connect: Al igual que realizamos una conexión por medio de telnet o netcat, este comando nos permite conectarnos a un host remoto y enviar ficheros si es lo que deseamos, también soporta SSL si se le indica la opción -s

- msf> connect 192.168.1.34 23

- exploit: Comando utilizado para realizar la ejecución del exploit cargado en el contexto de la consola.

- run: Comando utilizado para realizar la ejecución del módulo/auxiliary cargado en el contexto de la consola.

- irb: Permite ejecutar el intérprete de Ruby para metasploit, de este modo se pueden ingresar comandos y crear scripts al vuelo, esta característica es muy interesante para conocer la estructura interna del framework.

- jobs: Se trata de módulos que se encuentran en ejecución en "background" este comando permite listar y terminar comandos existentes.

- load: Permite cargar un plugin desde el directorio de plugins ubicado en la ruta de instalación, recibe como parámetro el nombre del plugin.

- unload: Descarga un plugin cargado, recibe como parámetro el nombre del plugin a descargar.

- loadpath: Trata de cargar un directorio donde se encuentran ubicados módulos, plugins o exploits externos al framework, de esta forma podemos tener exploits, payloads, etc. en un directorio independiente.

- resource: Carga un fichero de script que es posteriormente utilizado por algún exploit o modulo que depende de él.

- route: Permite establecer las tablas de enrutamiento de las sesiones de Metasploit generadas. Funciona similar al comando route de Linux, permite adicionar subredes, máscaras de red y gateways.

- info: Despliega información adicional de un módulo o exploit seleccionado anteriormente en la consola, incluyendo todas las opciones, objetivos y otra información.

- set: Permite establecer opciones del módulo o exploit seleccionado con el fin de suministrar los datos necesarios para su correcta ejecución.

- unset: Elimina el valor actual de una variable del exploit o módulo en uso.

- sessions: Permite listar, interactuar y terminar sesiones generadas por módulos o exploits, estas sesiones pueden ser consolas a máquinas remotas VNC, etc. con la opción -l se pueden listar las sessiones generadas, -i <number> permite iniciar la interacción con el número de consola establecido.

- search: permite ejecutar una búsqueda basada en expresiones regulares con un texto que pueda coincidir con el nombre de un módulo o exploit.

- show: Permite mostrar las diferentes opciones para módulos, exploits y payloads.

- msf> show auxiliary

- msf> show exploits

- setg: Permite definir variables globales que serán empleadas por todos los módulos o exploits cargados, de esta forma es posible definir variables bastante comunes como LHOST, RHOST, LPORT, RPORT, etc. en una única interacción con la consola sin escribir lo mismo una y otra vez.

- save: Permite almacenar de forma permanente las variables globales establecidas con el comando setg y las variables específicas de cada exploit en uso.

- use: Permite establecer el exploit o modulo a usar en la consola de Metasploit.

2.13. WINBOX

Es una herramienta se utiliza propiamente para administrar firewall de Mikrotik usando una interfaz gráfica, este software permite realizar conexiones FTP, Telnet y SSH. (Anrrango, 2014)

Capítulo 3.

3. Análisis de Resultados.

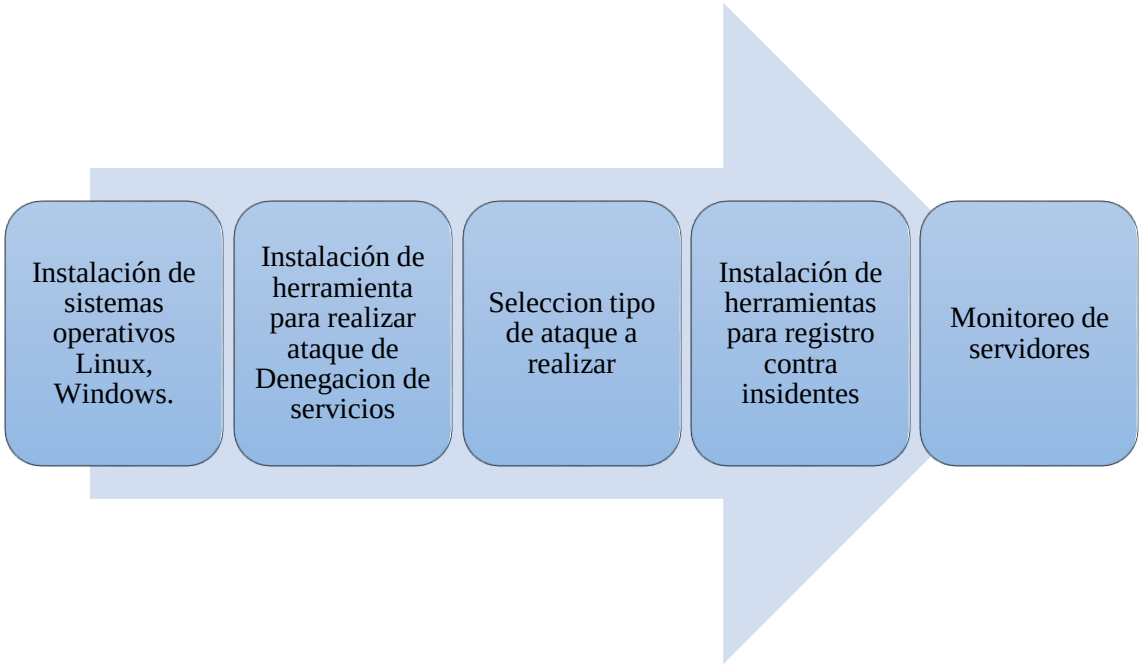

Figura 2: Pasos seguir desarrollo DoS
Fuente: Elaboración del autor

Procedimiento:

Sistemas operativos: para ejecutar el ataque de Denegación de servicios se trabajó sobre los sistemas operativos Linux (Ubuntu 18.4) y Windows (Windows Server 2012).

Sistema de ataque de Denegación de servicios: Para realizar el ataque se utilizó la herramienta Kali Linux que sirve para generar un ataque de Denegación de servicios a través de envió de paquetes mediante exploits se seleccionó el ataque que se utilizara es ***Flood*** o también conocido como ataque de inundación que consiste en bombardear un sistema con un flujo continuo de tráfico que intenta consumir todos los recursos y el Ancho de Banda de la red del sistema, de esta manera evitar que los usuarios tengan acceso a determinado servicio.

Herramientas: Para la práctica se utilizó Webmin e Apache2 servidores para Linux y Windows server Internet Information Service (IIS) para Windows, para el registro y

control de los incidentes después de cada ataque realizado, con el cual se contó con un ambiente de producción real orientado a los incidentes que causara los ataques a cada servidor atacado.

Sistema de monitoreo: Para realizar el seguimiento del consumo de recursos enfocado a cada servidor en Linux se realizó mediante Webmin ya que posee dentro del mismo un sistema de monitoreo llamado **System Information** que nos permite conocer rendimiento y el estado de memoria CPU, para Windows se utilizó el sistema de monitoreo Internet Information Service (IIS) el ***Monitor de Rendimiento*** que se encuentra en las ***Herramientas de Supervisión*** que nos permite ver el rendimiento del servidor.

Desarrollo:

3.1. Instalación de la Herramienta VirtualBox, Servidor Windows.

Para el presente trabajo se utilizó la herramienta de virtualización Oracle VM VirtualBox versión 5.2.2 r119230 (Qt5.6.2).

Luego de la instalación de la herramienta de virtualización se procedió a la instalación de las máquinas virtuales tanto para Windows como Linux.

Instalación de la máquina virtual Windows (Windows Server 2012) con las siguientes características:

- Nombre Servidor Windows
- Sistema operativo Windows 2012 (64 bit)
- Memoria 3608 MB
- Memoria de video 128MB

3.1.1. Configuración de Red LAN Servidor Windows.

Para establecer la configuración de la red de este servidor virtual se procede a configurar en modo adaptador puente entre la tarjeta de red virtual y la tarjeta de red física del servidor, de esta forma obtenemos un direccionamiento ip en el mismo ámbito de la red local.

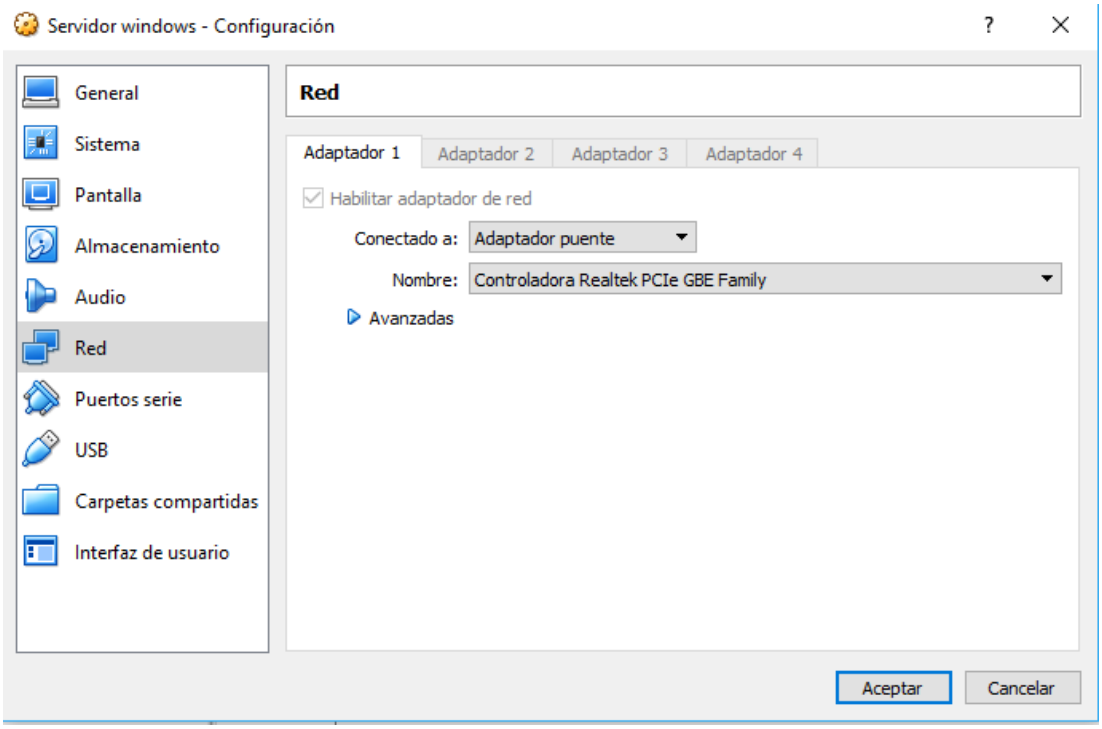

Figura 3: Configuración adaptador puente Servidor Windows.

Fuente: VirtualBox

3.1.2 Configuración de la Red WAN Servidor Windows.

Para realizar las pruebas en una ip publica se utilizó un firewall MikroTik el cual se administra mediante la herramienta Winbox en donde se realizó la configuración de redireccionamiento de puertos de ambos servidores para publicar los sitios (ejemplo) con la ip pública.

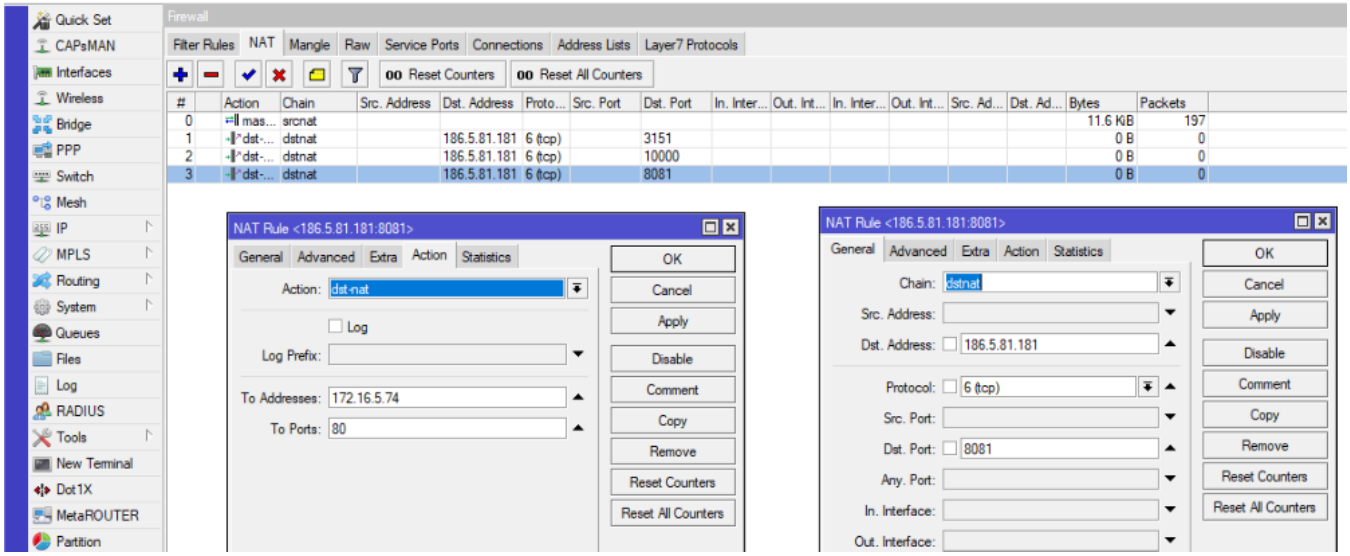

Figura 4: Configuración NAT Servidor Windows.
Fuente: Winbox-MikroTik

3.1.3 Levantamiento de Servidor Windows (Windows Server 2012)

Se procede a verificar la conexión a internet y verificar las direcciones ip de la máquina para levantar el servidor y realizar las configuraciones.

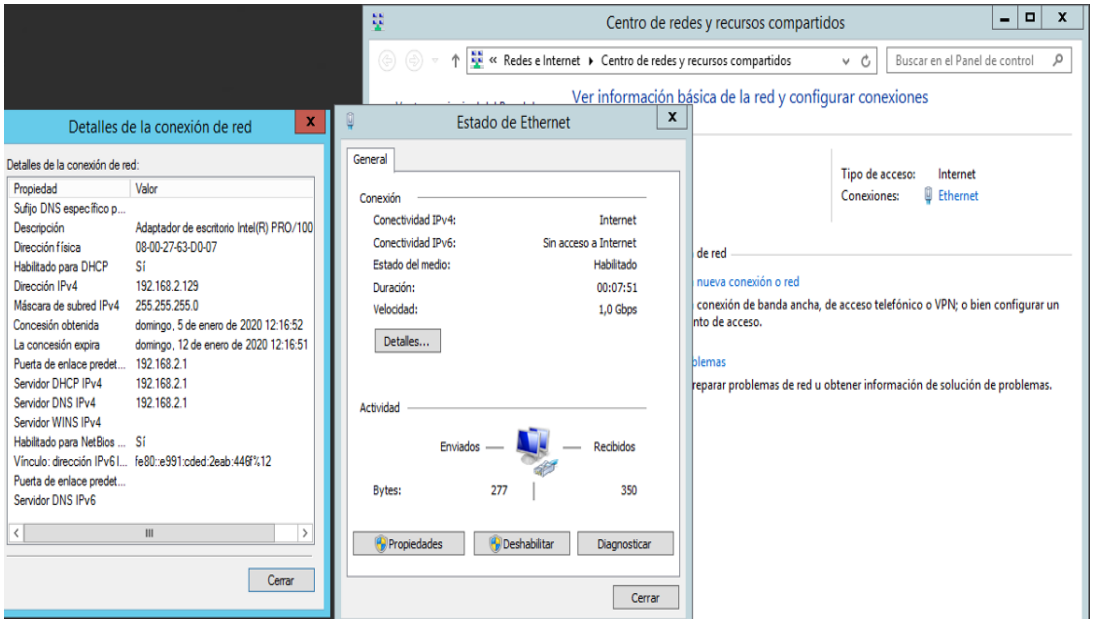

Figura 5: Verificacion de la direccion ip Servidor Windows Server 2012.
Fuente: Windows Server 2012

Se agrega los roles y caracteristicas Internet Information Service (IIS) para el Servidor web y se procedio a instalarlo.

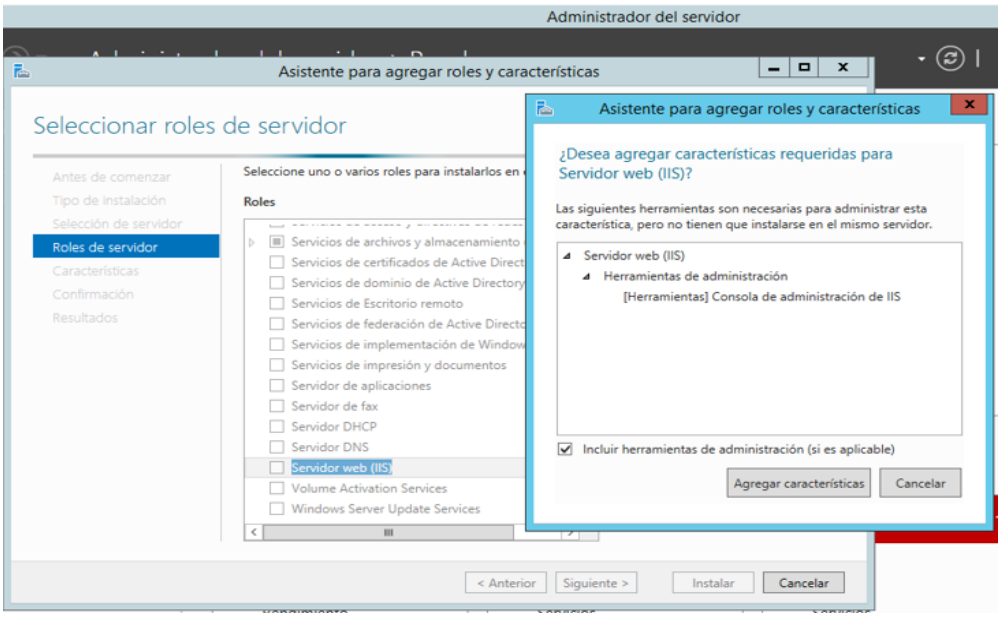

Figura 6: Instalación Roles y Características Internet Information Service (IIS.)
Fuente: Windows Server 2012

Verificación de Ingreso al Servidor Web antes de la instalación en la imagen se observa que nos re direccionara al buscador Web tanto ingresando por la dirección ip o como por Local Host.

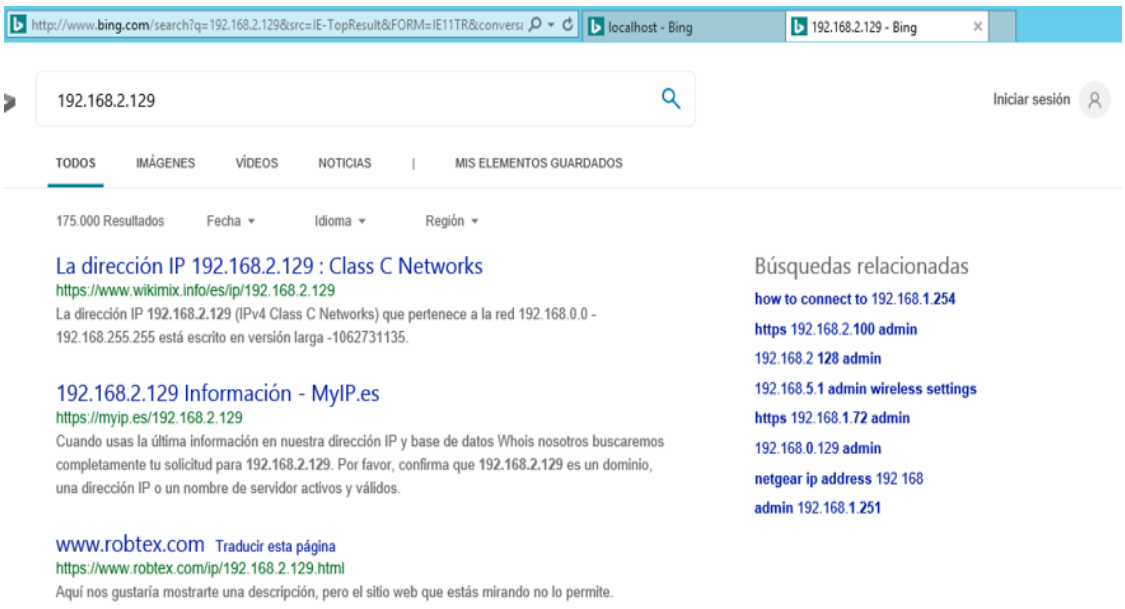

Figura 7: Verificación de ingreso a la ip local.
Fuente: www.bing.com

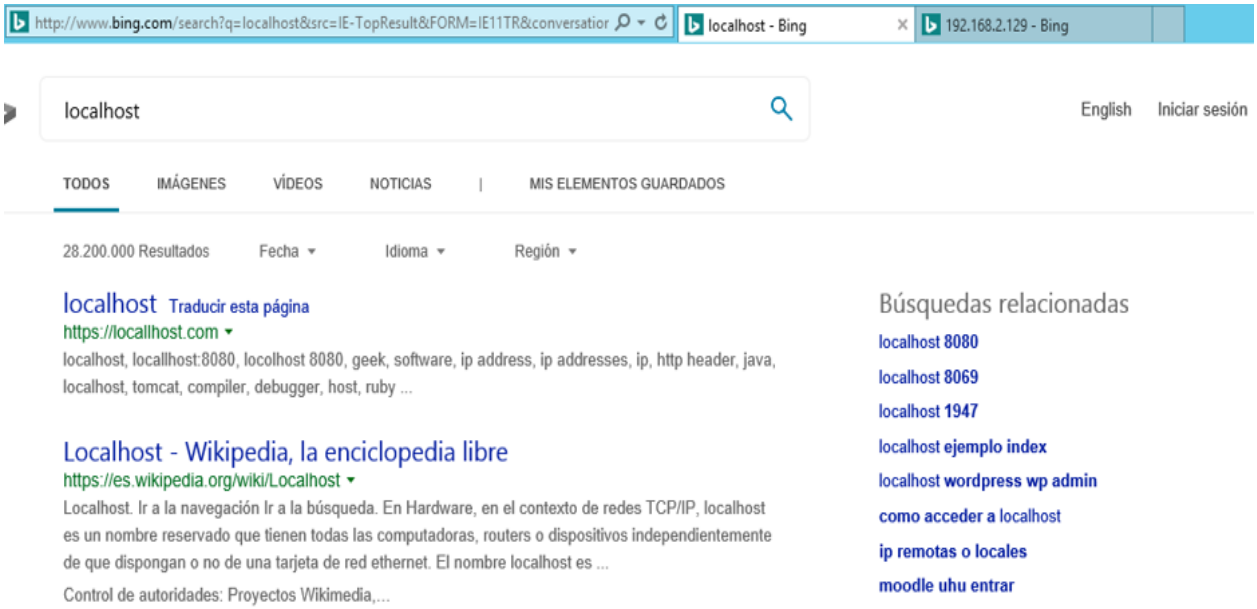

Figura 8: Verificación de ingreso a Local Host.
Fuente: www.bing.com

Instalación de los roles y características del servidor web Internet Information Service (IIS).

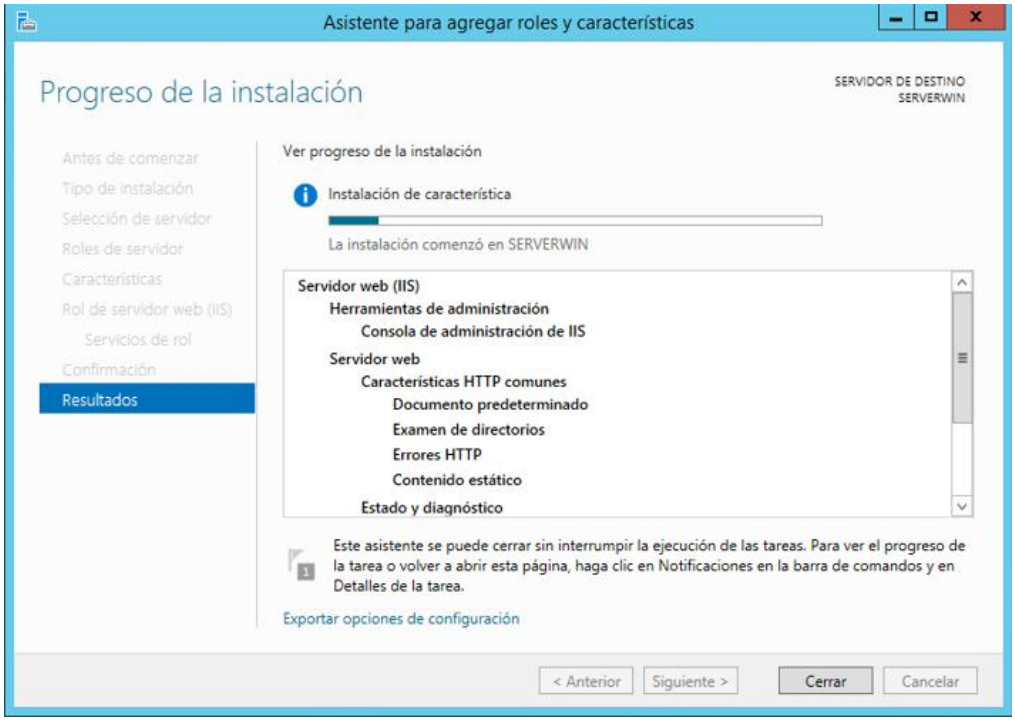

Figura 9 Instalación de Roles y Características de Internet Information Service (IIS).
Fuente: Windows Server 2012.

Luego se verifica si el servidor web está en funcionamiento cargando mediante la dirección ip o localmente (Local Host)

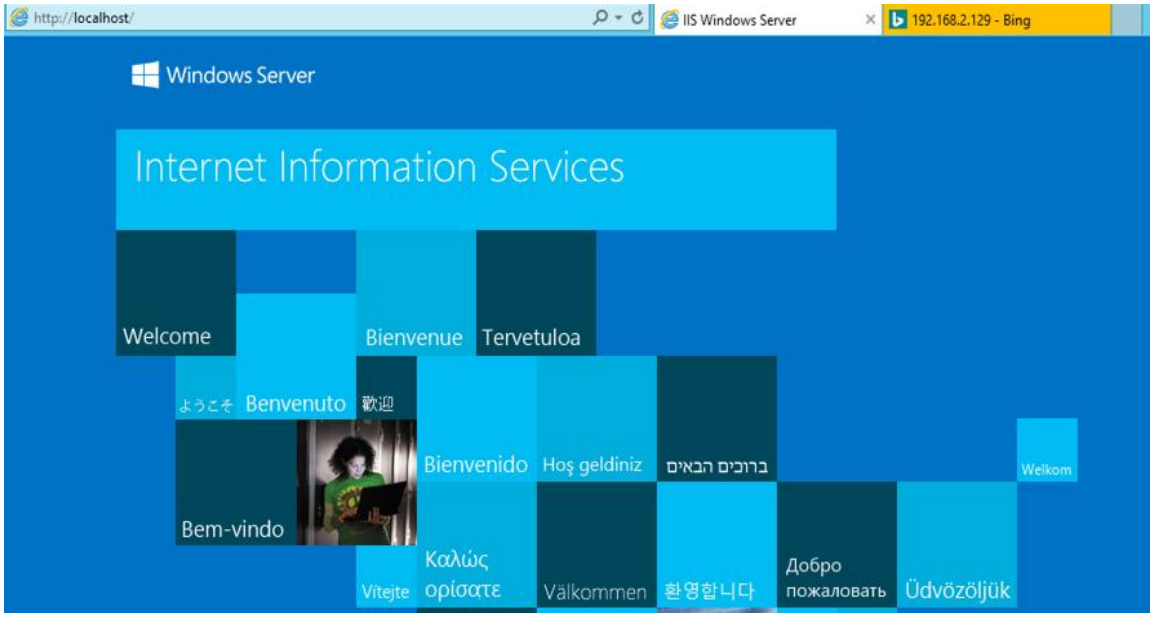

Figura 10: Navegación de Servidor Windows Levantado desde Local Host.
Fuente: Internet Information Services (Windows Server 2012).

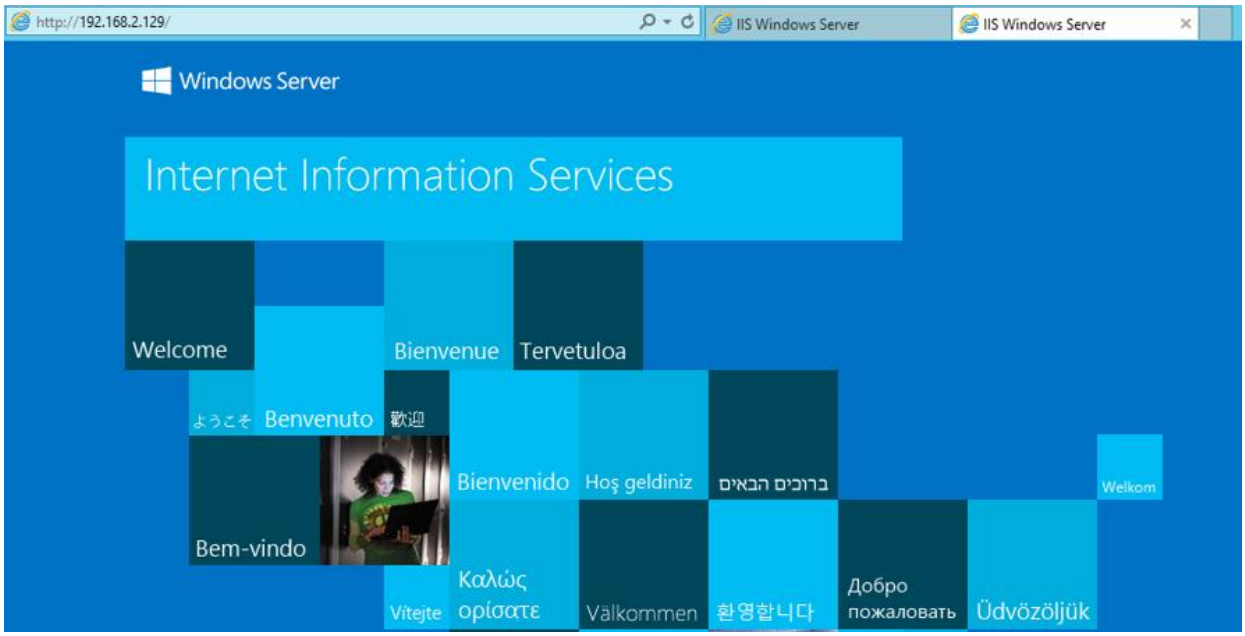

Figura 11: Navegación de Servidor Windows Levantado desde dirección ip local.
Fuente: Internet Information Services (Windows Server 2012).

Luego se procede a levantar el servidor y se cargo un ejemplo al servidor para posteriormente realizar el estudio de Denegacion de Servicios (DoS).

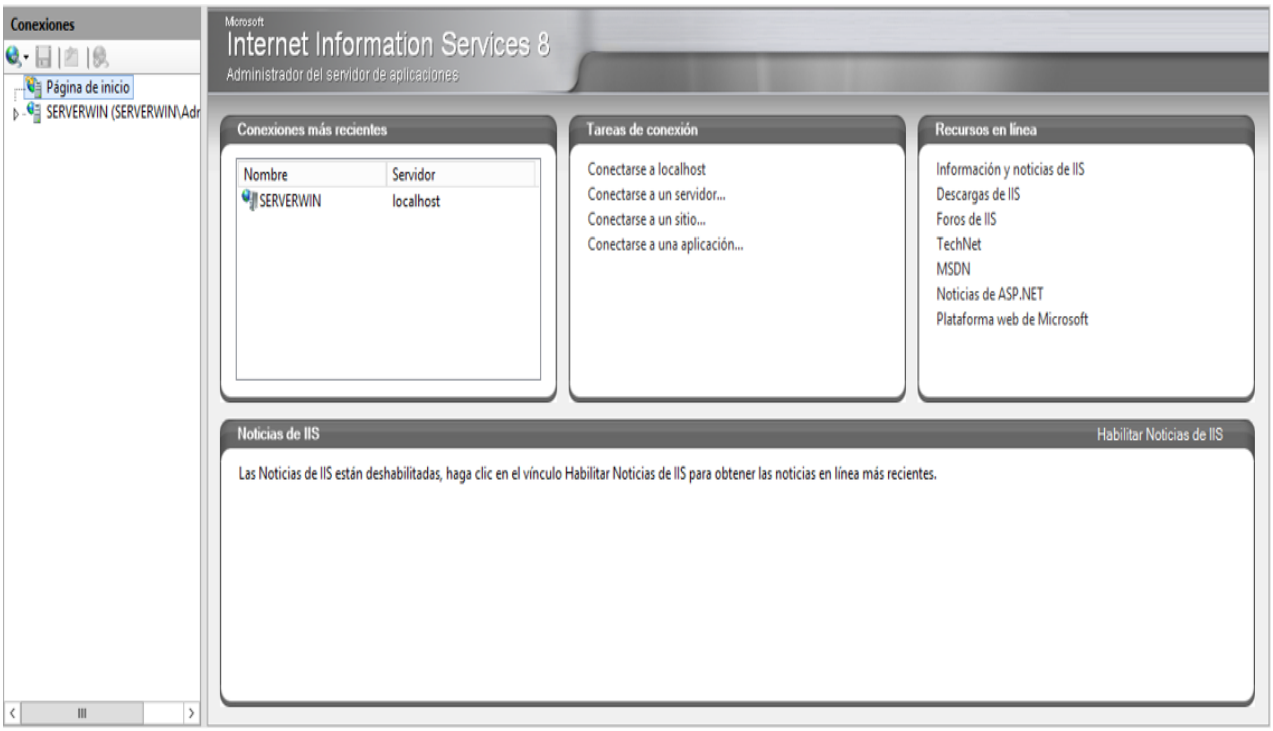

Figura 12: Configuración de Servidor Windows (SERVERWIN).
Fuente: Internet Information Services (Windows Server 2012).

Se subió la página de Ejemplo para en lo posterior atacar el servidor Windows.

Figura 13: Navegación de Ejemplo mediante dirección localhost.
Fuente: Local Host Windows Server 2012.

3.2. Instalación de la máquina virtual Ubuntu (18.04)

Segundo, se instaló la máquina virtual en Linux con las siguientes características:

- Nombre: Servidor Linux
- Sistema operativo: Ubuntu 18.4 (64 bit)
- Memoria 5079 MB
- Memoria de video 16 MB

3.2.1 Configuración de red LAN servidor Linux

Para establecer la configuración de la red de este servidor virtual se procede a configurar en modo adaptador puente entre la tarjeta de red virtual y la tarjeta de red física del servidor, de esta forma obtenemos un direccionamiento ip en el mismo ámbito de la red local.

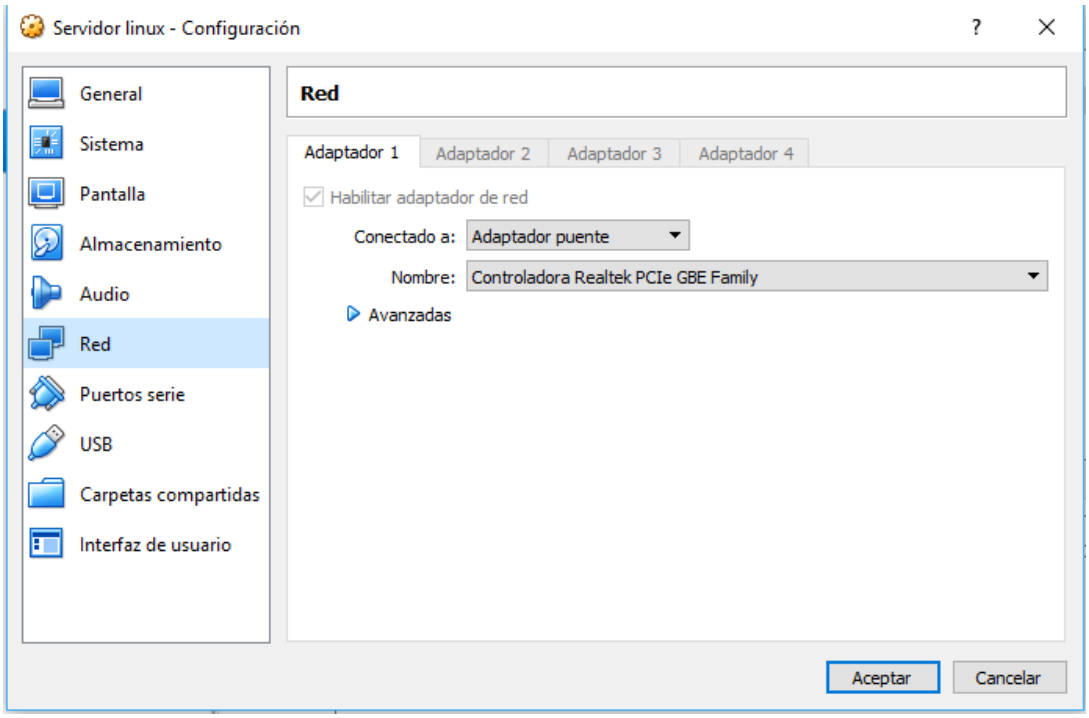

Figura 14: Configuración adaptador puente Servidor Linux.
Fuente: VirtualBox

3.2.2 Configuración de la Red WAN Servidor Linux

Para realizar las pruebas en una ip publica se utilizó un firewall Mikrotik el cual se administrar mediante la herramienta Winbox en donde se realizó la configuración de redireccionamiento de puertos de ambos servidores para publicar los sitios (ejemplo) con la ip pública.

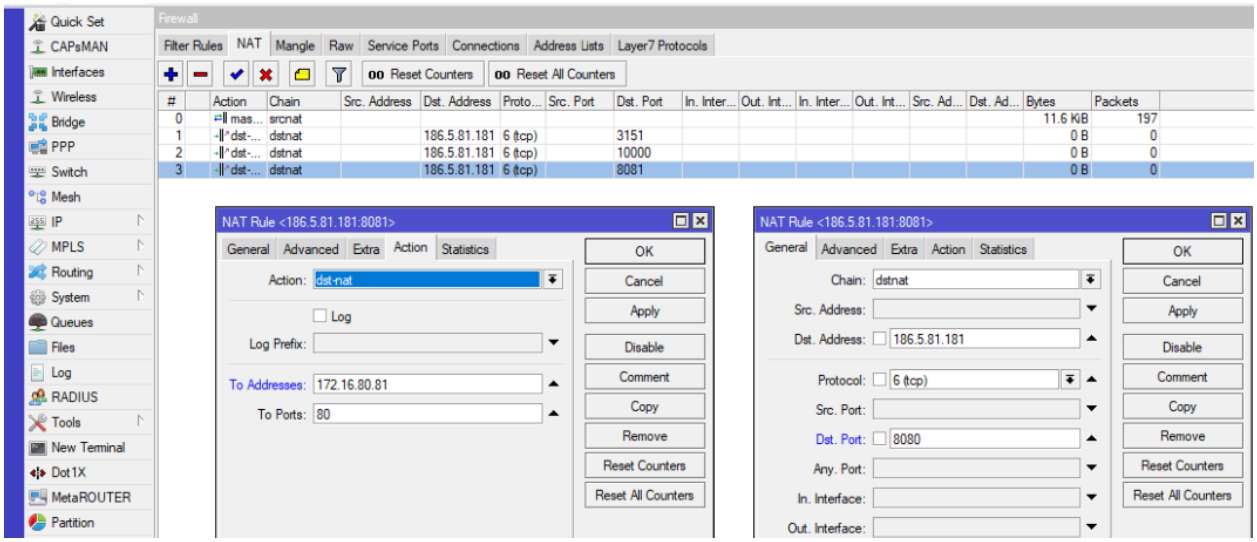

Figura 15: Configuración NAT Servidor Linux.
Fuente: Winbox-MikroTik

3.2.3 Levantamiento de Servidor Linux Ubuntu 18.4 (Apache2)

Se procede a la instalación del servidor (Apache2) con el comando ***sudo apt-get install apache2*** este comando instalo todos los drivers necesarios para el servidor web para poder utilizarlo.

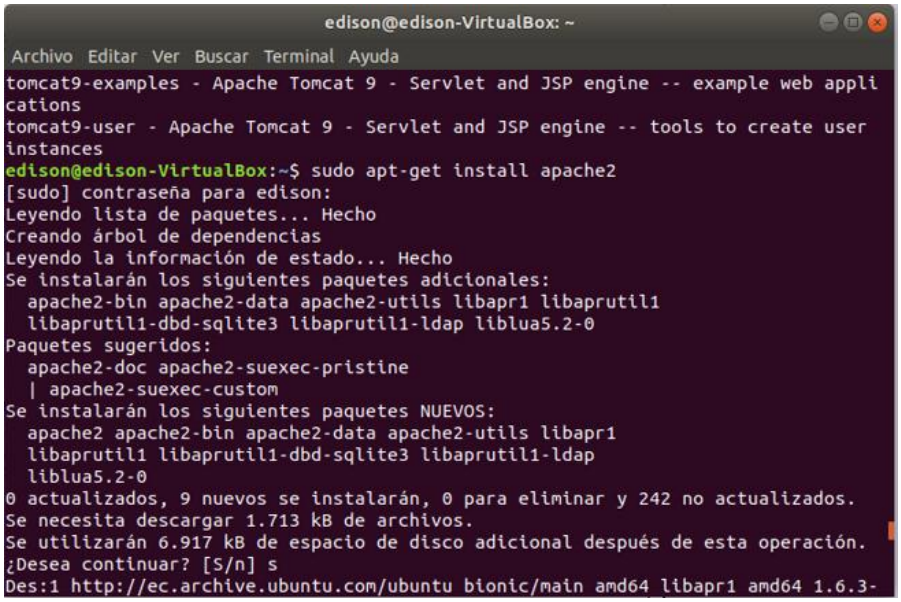

Figura 16: Instalación del Servidor Apache2.
Fuente: Terminal Ubuntu 18.04

Luego, Se procede a verificar la conexión a internet y las direcciones ip de la máquina para levantar el servidor.

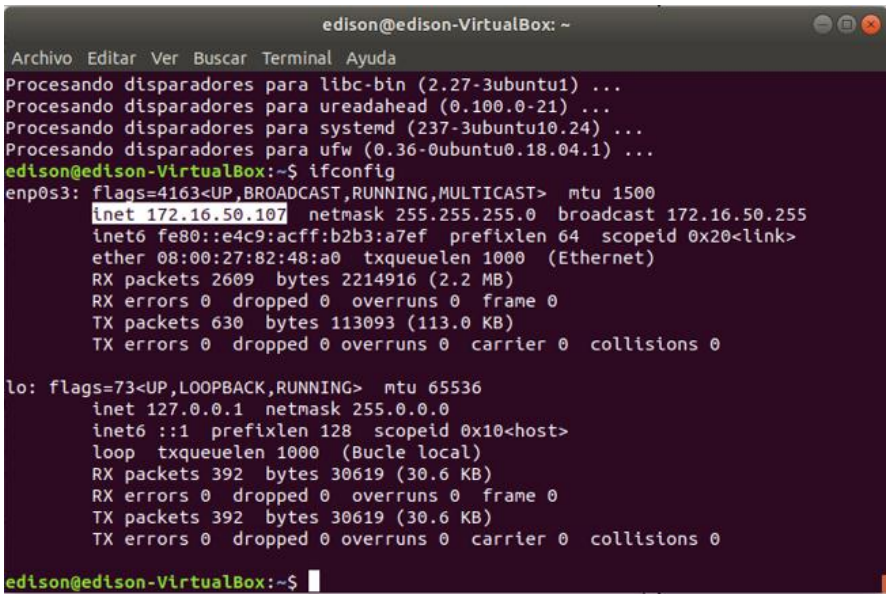

Figura 17: Verificación de la ip del Servidor Ubuntu 18.04
Fuente: Terminal Ubuntu 18.04

Se procede a levantar el servidor y cargar el ejemplo para en lo posterior realizar el ataque al servidor Linux.

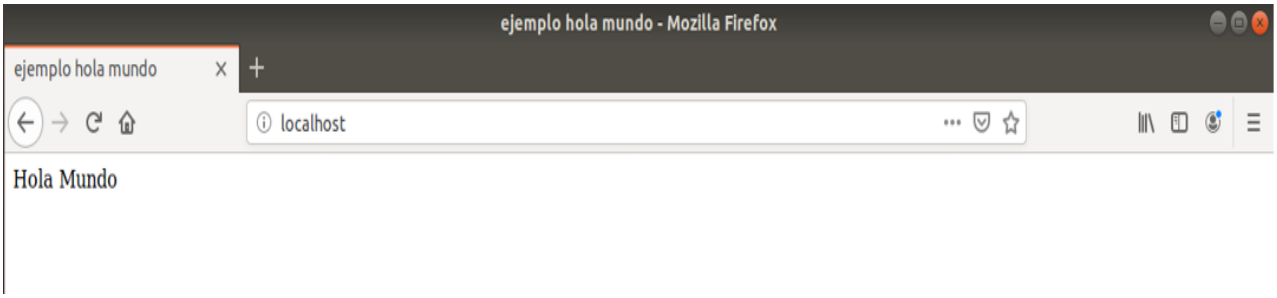

Figura 18: Navegación de Ejemplo mediante localhost.
Fuente: Local Host Ubuntu 18.04

3.2.4 Levantamiento de Servidor Linux Ubuntu 18.4 (Webmin)

Se procede a la instalación del servidor (Webmin) con el comando ***sudo apt install Webmin*** este comando instalo todos los drivers necesarios para el servidor web y poder utilizarlo.

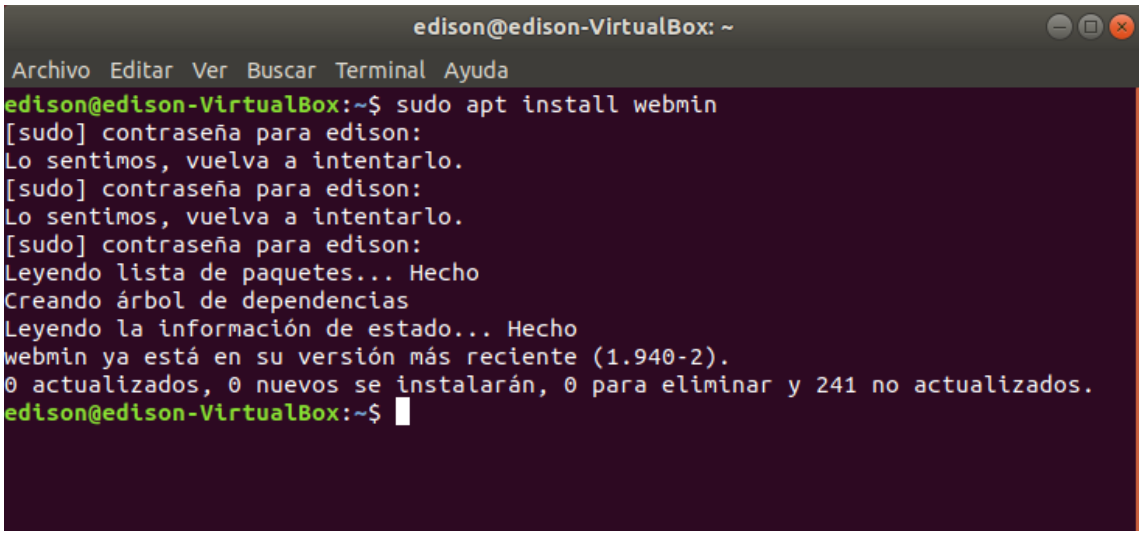

Figura 19: Instalación Webmin
Fuente: Terminal Ubuntu 18.04

Luego, Se procede a verificar la conexión a internet y las direcciones ip de la máquina para levantar el servidor.

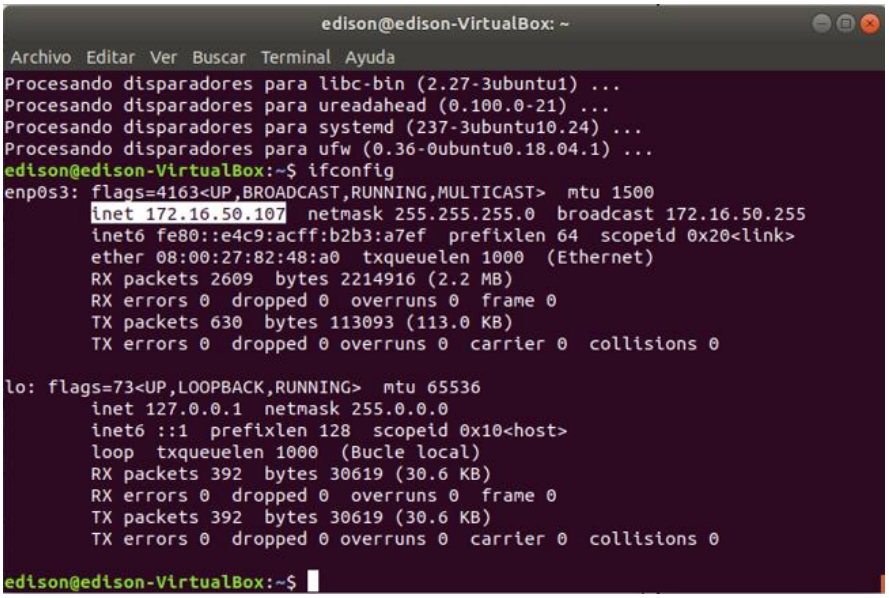

Figura 20: Verificación de la ip del servidor Ubuntu 18.04
Fuente: Terminal Ubuntu 18.04

Se procede a levantar los servidores con el puerto respectivo de Webmin, para verificar si se levantó los Servicios y para en lo posterior realizar el ataque al servidor Webmin.

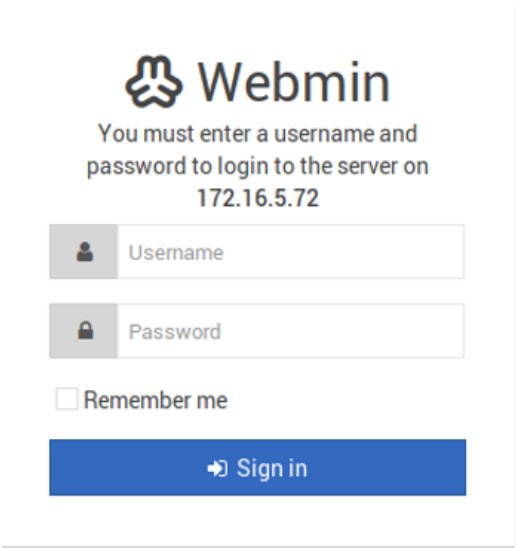

Figura 21: Verificación de Servidor Webmin este activo
Fuente: Webmin

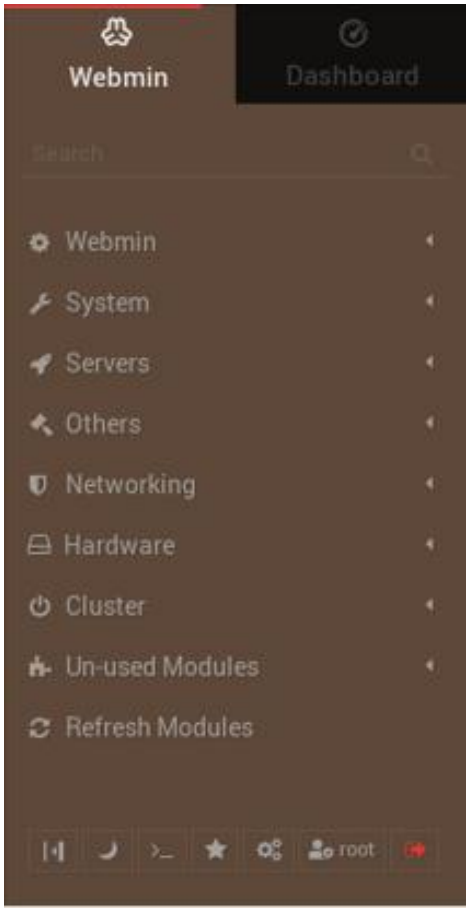

Figura 22: Menú Webmin
Fuente: Webmin

3.3.Instalación de la Herramienta Kali Linux.

Instalación de la herramienta Kali Linux en VirtualBox con un sistema operativo Linux en otra máquina configurándolo de la siguiente manera:

- Nombre: Kali Linux
- Sistema Operativo: Linux 2.6 (64 bit)
- Memoria 1024 MB
- Memoria de video 16 MB
- Almacenamiento 16 GB

Finalizado las configuraciones de la instalación de la herramienta Kali Linux se procede a instalar en la máquina virtual la imagen de Kali Linux.

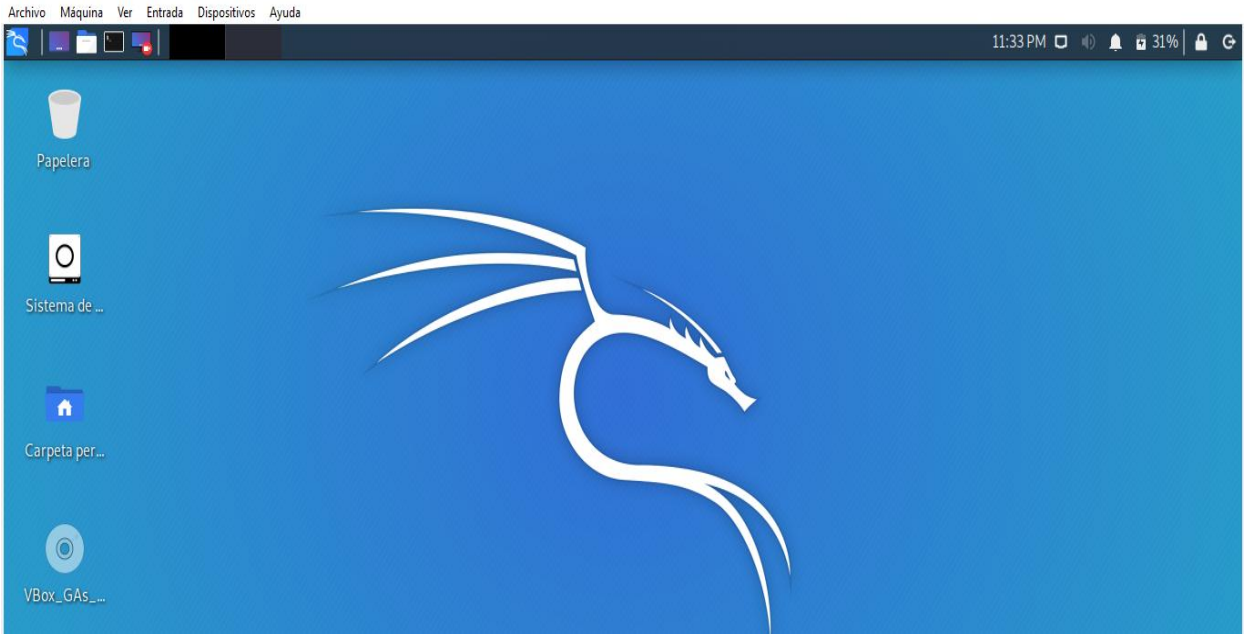

Figura 23: Herramienta Kali Linux GUI
Fuente: Imagen escritorio Kali Linux

3.4. Pasos a seguir para realizar un ataque mediante la consola Metasploit en Kali Linux:

a) Ingresar al terminal Metasploit

b) Ejecutar el comando ***msfconsole*** para ingresar a la consola ***msf5*** de Matasploit.

c) Se ingresa con el comando ***use auxiliary/dos/tcp/synflood*** que es donde se encuentra el archivo para realizar el ataque ***Flood*** o también conocido como **ataque de inundación** que consiste en bombardear un sistema con un flujo continuo de tráfico que intenta consumir todos los recursos y el Ancho de Banda de la red del sistema.

d) Luego se ingresó a la dirección ip a la que se quiere atacar con el comando ***set RHOST 172.0.0.0*** **en** casos cuando se utiliza direcciones ip publicas también se utiliza el comando ***set RPORT*** **8080** para especificar el puerto en el cual se encuentra dicha red, se puede utilizar el programa Wireshark que muestra el tráfico de la red y también los

paquetes que lleva cada dirección ip y dentro de cada paquete se puede ingresar y ver el puerto que se utiliza.

e) Ya obtenido todo esto se precede a ejecutar el ataque como se lo conoce en Kali Linux "Attack" con el comando ***exploit.***

3.5. Diagrama-Ataque Red LAN

Figura 24: Diagrama ataque red LAN.
Fuente: (Azamar, 2017)

3.6.Diagrama-Ataque Red WAN

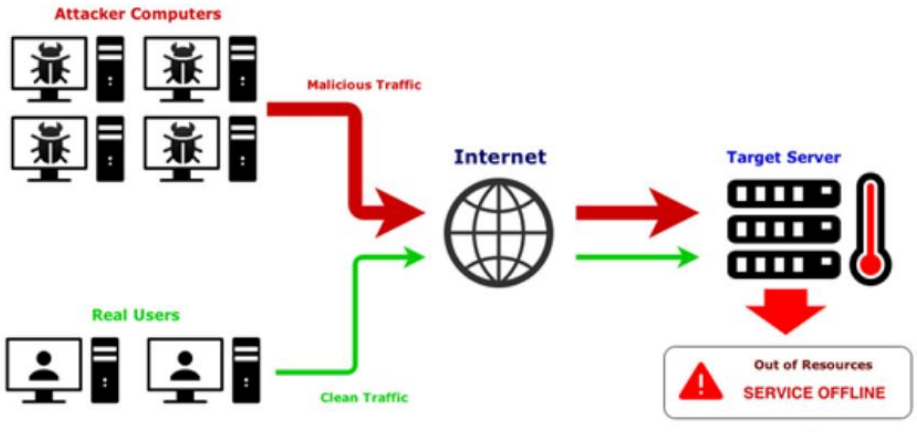

Figura 25: Diagrama Red WAN.
Fuente: (NEXTVISION, 2018)

3.7.Ataque de Denegación de Servicios (DoS) Mediante Kali Linux utilizando Metasploit.

3.7.1. Primer ataque realizado a el servidor Windows (Windows Server 2012) Localmente red LAN

El servidor esta inicializado por el cual se comprueba mediante la dirección ip local para verificar que este navegando.

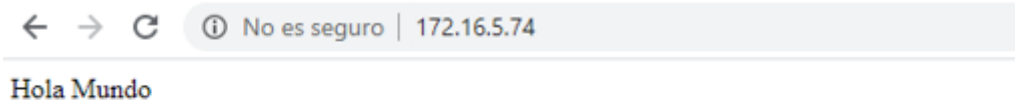

Figura 26: Verificación de Navegación de Servidor Windows mediante dirección ip local.
Fuente: Navegación ip local Windows Server 2012

Siguiendo los pasos ya descritos anteriormente se procedió a realizar el ataque al servidor Windows (Windows server 2012)

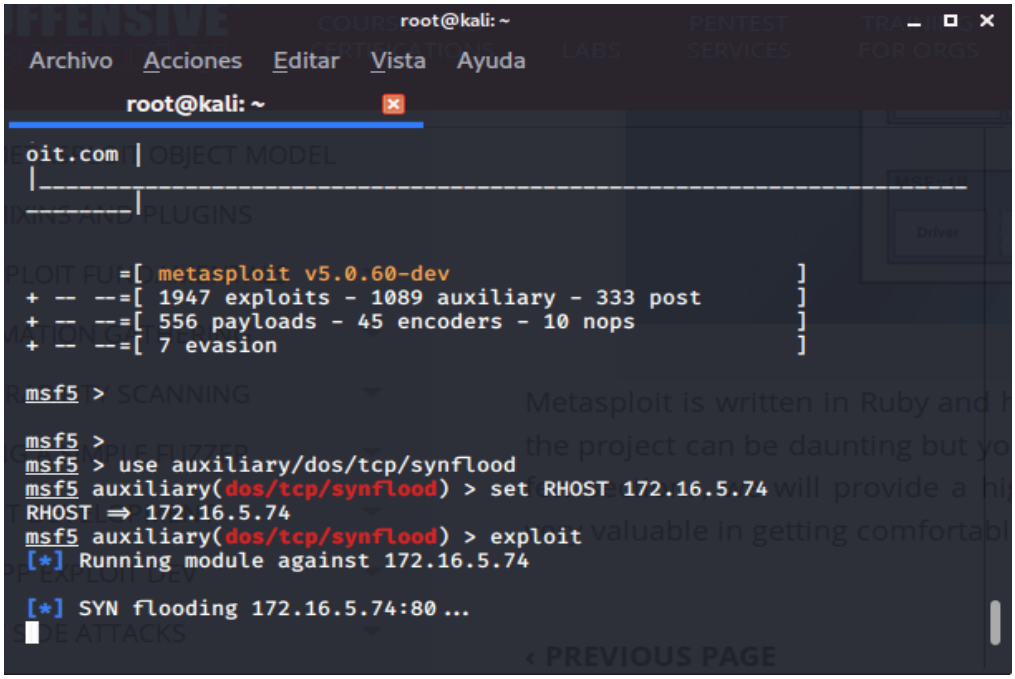

Figura 27: Ataque Realizado a Servidor Windows mediante Metasploit en Kali Linux.
Fuente: msfConsole Kali Linux

Se verifica que los servicios hayan caído del servidor Windows (Windows server 2012)

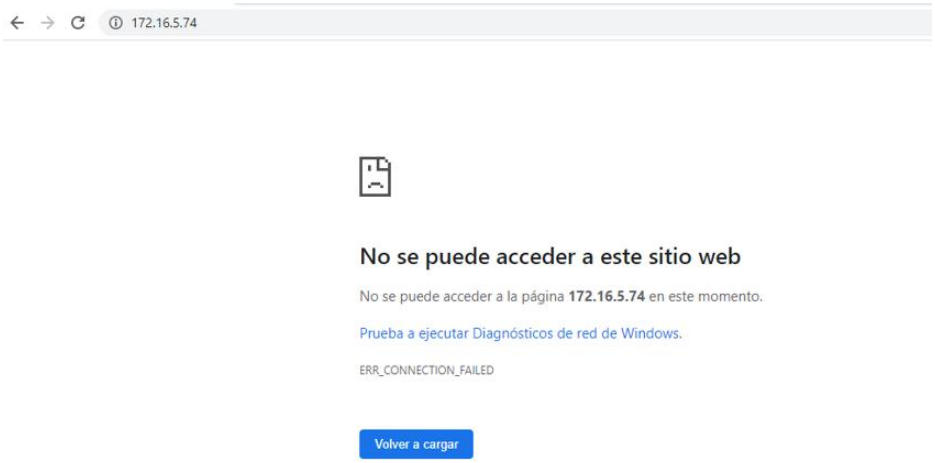

Figura 28: Verificación de Caída del Servidor Navegando desde la dirección ip local.
Fuente: Navegación ip local Windows Server 2012

Se procede a parar el ataque con las teclas ***Ctrl c*** y verificar si nuevamente se levanta el servicio de la página de ejemplo.

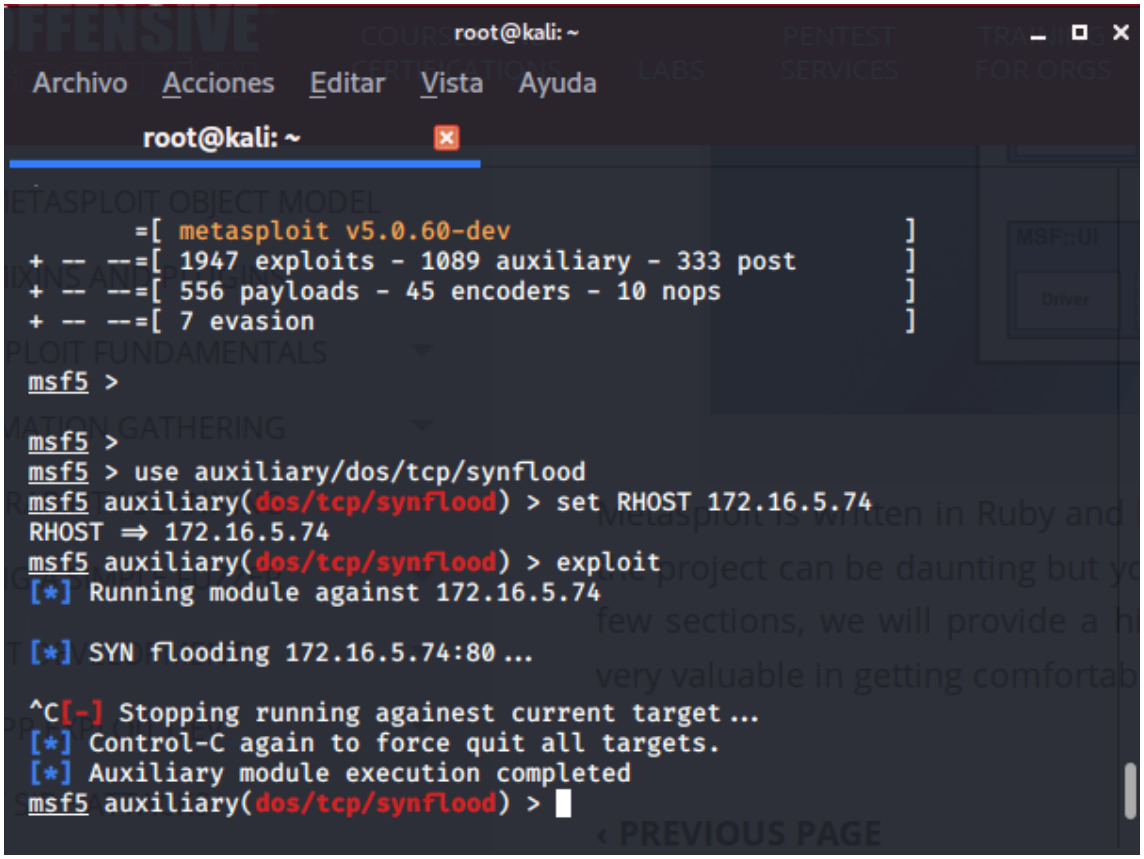

Figura 29: Detención del Ataque de Metasploit en el Servidor Windows.
Fuente: msfConsole Kali Linux

Verificar que los servicios estén levantados nuevamente para asegurar que el ataque se haya detenido.

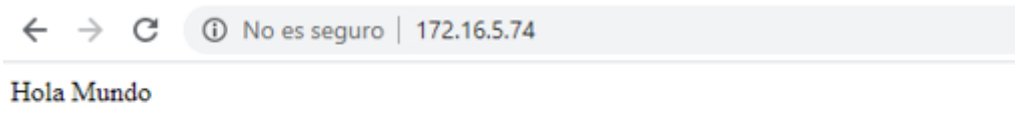

Figura 30: Verificación de servicio activo en el servidor Windows después de la detención del ataque.
Fuente: Navegación ip local Windows Server 2012

3.7.2. Segundo ataque realizado al servidor Linux (Ubuntu 18.4)

Localmente red LAN

El servidor esta inicializado por el cual se comprueba mediante la dirección ip local para verificar que se esté navegando.

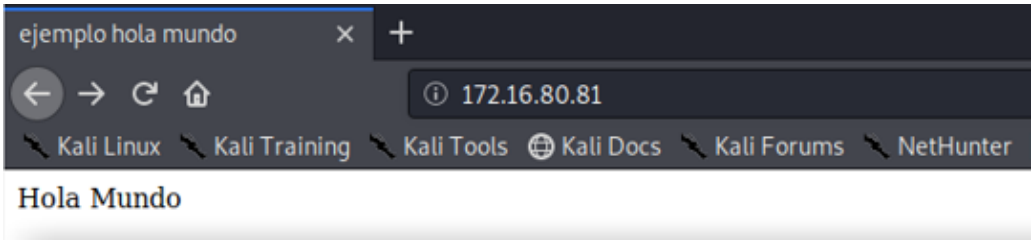

Figura 31: Verificación de Navegación de Servidor Linux mediante dirección ip local.
Fuente: Local Host Linux Ubuntu 18.04

Se procede a realizar el ataque mediante Metasploit en Kali Linux para detener el servicio del servidor de Linux

Figura 32: Ataque Realizado a Servidor Linux mediante Metasploit en Kali Linux.
Fuente: msfConsole Kali Linux

Luego, Se verificó que los servicios hayan caído del servidor navegando la dirección ip local.

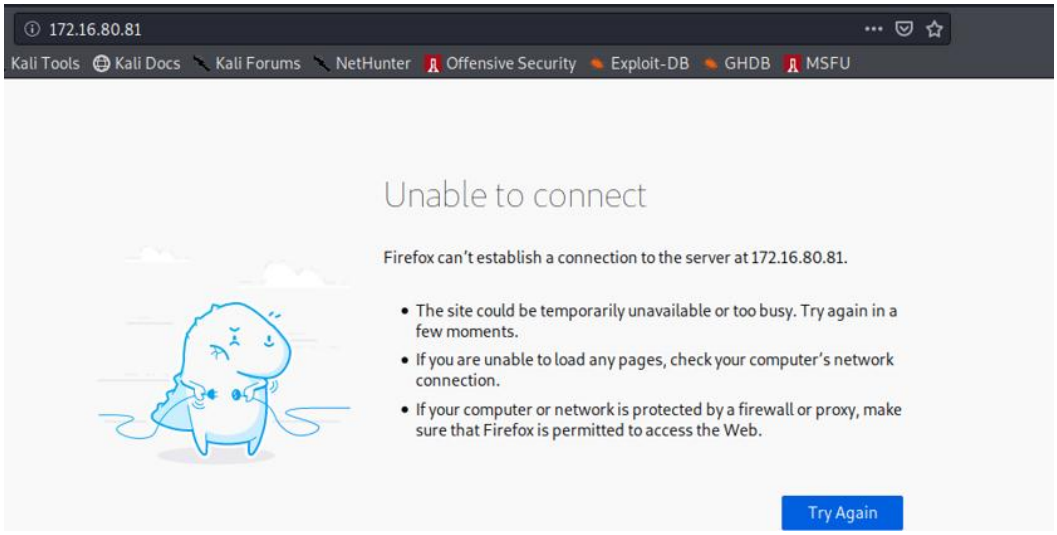

Figura 33: Verificación de Caída del Servidor Navegando desde la dirección ip local.
Fuente: Navegación ip local Linux Ubuntu 18.04

De igual forma a la anterior se procede a parar el ataque y verificar que el servicio se vuelva a levantar.

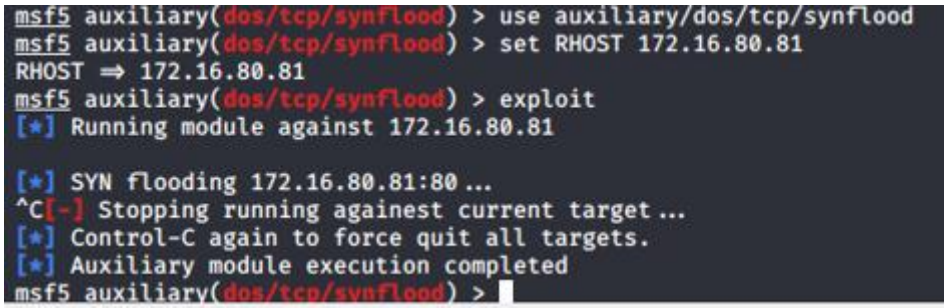

Figura 34: Detención del Ataque de Metasploit en el Servidor Linux.
Fuente: msfConsole Kali Linux

Se verificó que el servicio este activo nuevamente navegando desde la dirección ip local.

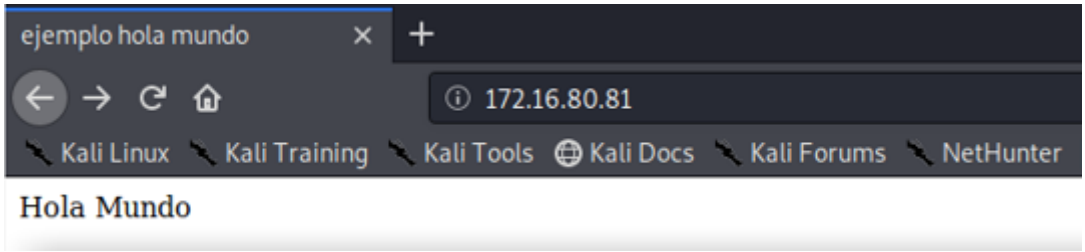

Figura 35: Verificación de servicio activo en servidor Linux después de la detención del ataque.
Fuente: Navegación ip local Linux Ubuntu 18.04

3.7.3. Tercer ataque realizado al servidor Windows (Windows Server 2012)

Red WAN con ip pública.

El servidor esta inicializado por el cual se comprobó mediante la dirección ip pública y el puerto activo.

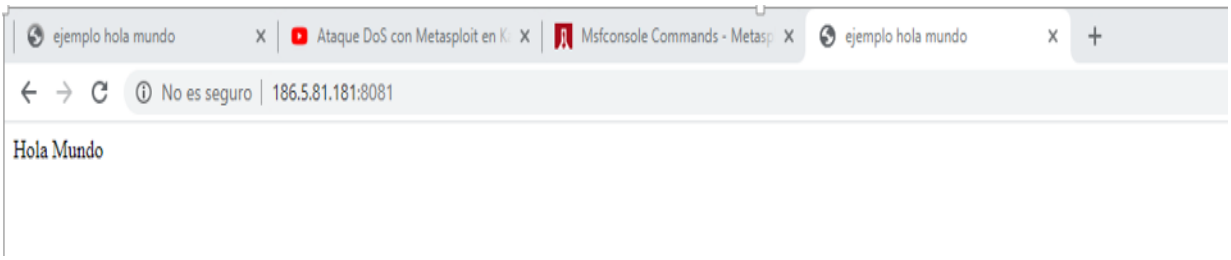

Figura 36: Verificación de navegación de servidor Windows mediante dirección ip pública.
Fuente: Navegación ip publica Windows Server 2012

Se Procede a realizar el ataque al servidor mediante la Consola Metasploit de la herramienta Kali Linux.

Para la ejecución de este ataque de los servidores publicados en una ubicación específica, fue atacado mediante Kali Linux desde otra ubicación para dar certeza de que el ataque funciono, es decir los servidores estuvieron en un punto A y el atacante en un punto B no definido.

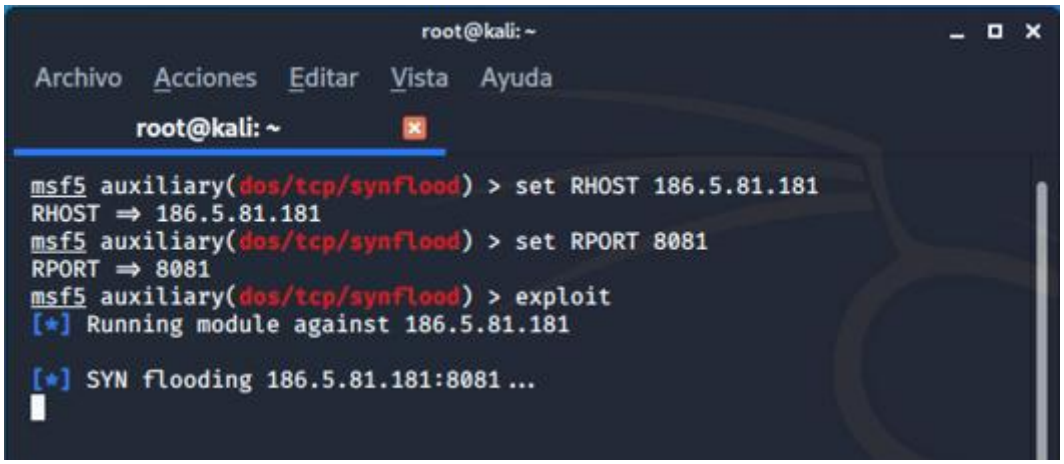

Figura 37: Ataque Realizado a Servidor Windows ip pública mediante Metasploit en Kali Linux.
Fuente: msfConsole Kali Linux

Se verifico que los servicios de la ip pública hayan caído navegando desde la ip pública y respectivo puerto.

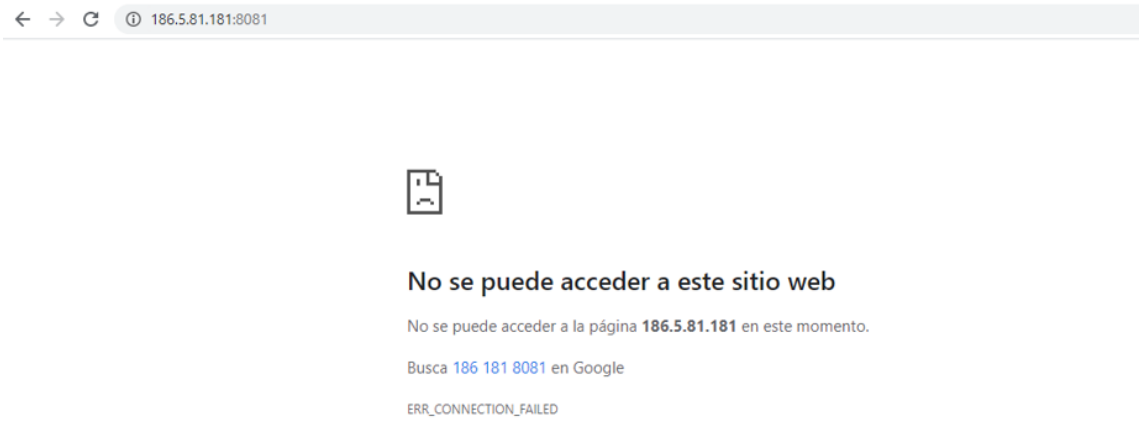

Figura 38: Verificación de caída del servidor Windows navegando desde la dirección ip pública.
Fuente: Navegación ip publica Windows Server 2012

Se detiene en lo posterior el ataque y se verifica si los servicios se vuelven a levantar del servidor web.

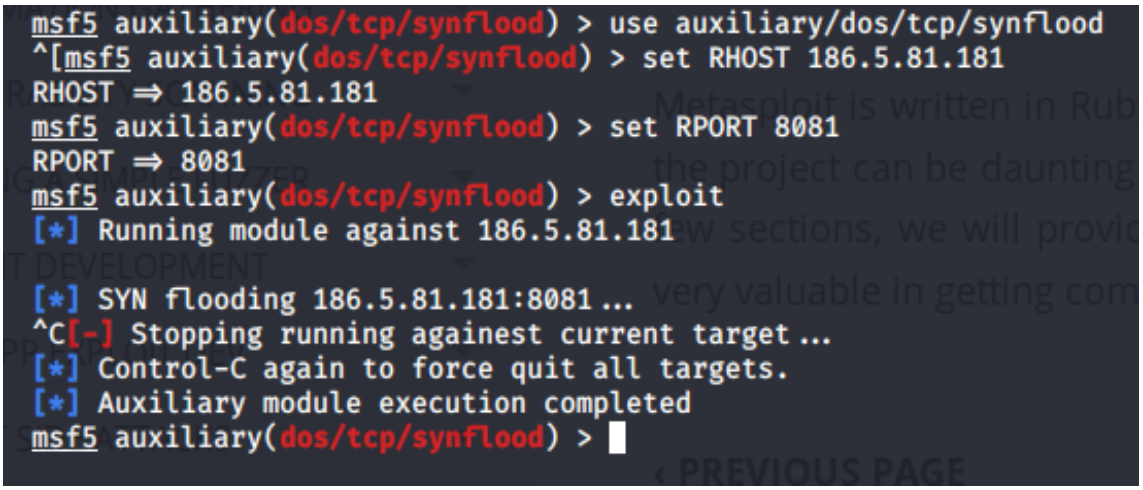

Figura 39: Detención del Ataque de Metasploit en el Servidor Windows.
Fuente: msfConsole Kali Linux

Se verifico que los servicios se hayan levantado nuevamente, navegando en la dirección ip pública.

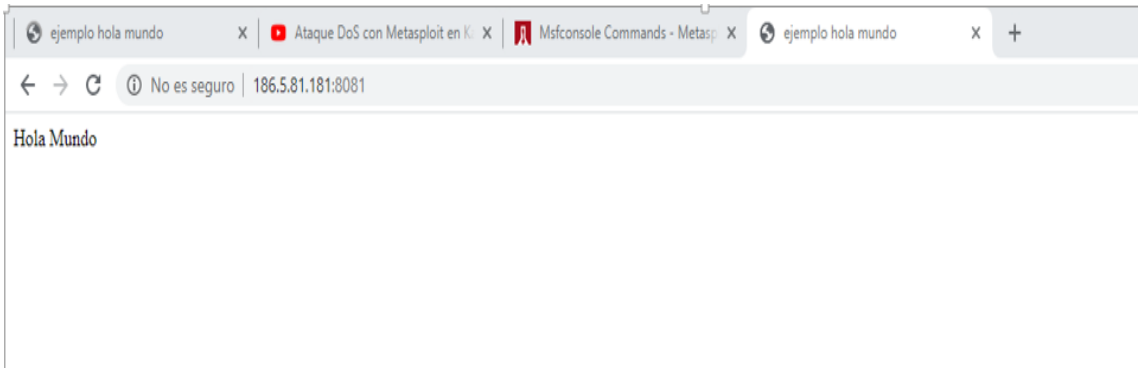

Figura 40: Verificación de servicio activo en servidor Windows después de la detención del ataque.
Fuente: Navegación ip publica Windows Server 2012

Por último, Se verifico cómo reacciona el servidor al momento de realizar el ataque monitoreando el servidor mediante el ***Monitor de Rendimiento*** que se encuentra en las ***Herramientas de Supervisión*** del servidor Windows (Windows Server 2012) obteniendo los siguientes resultados.

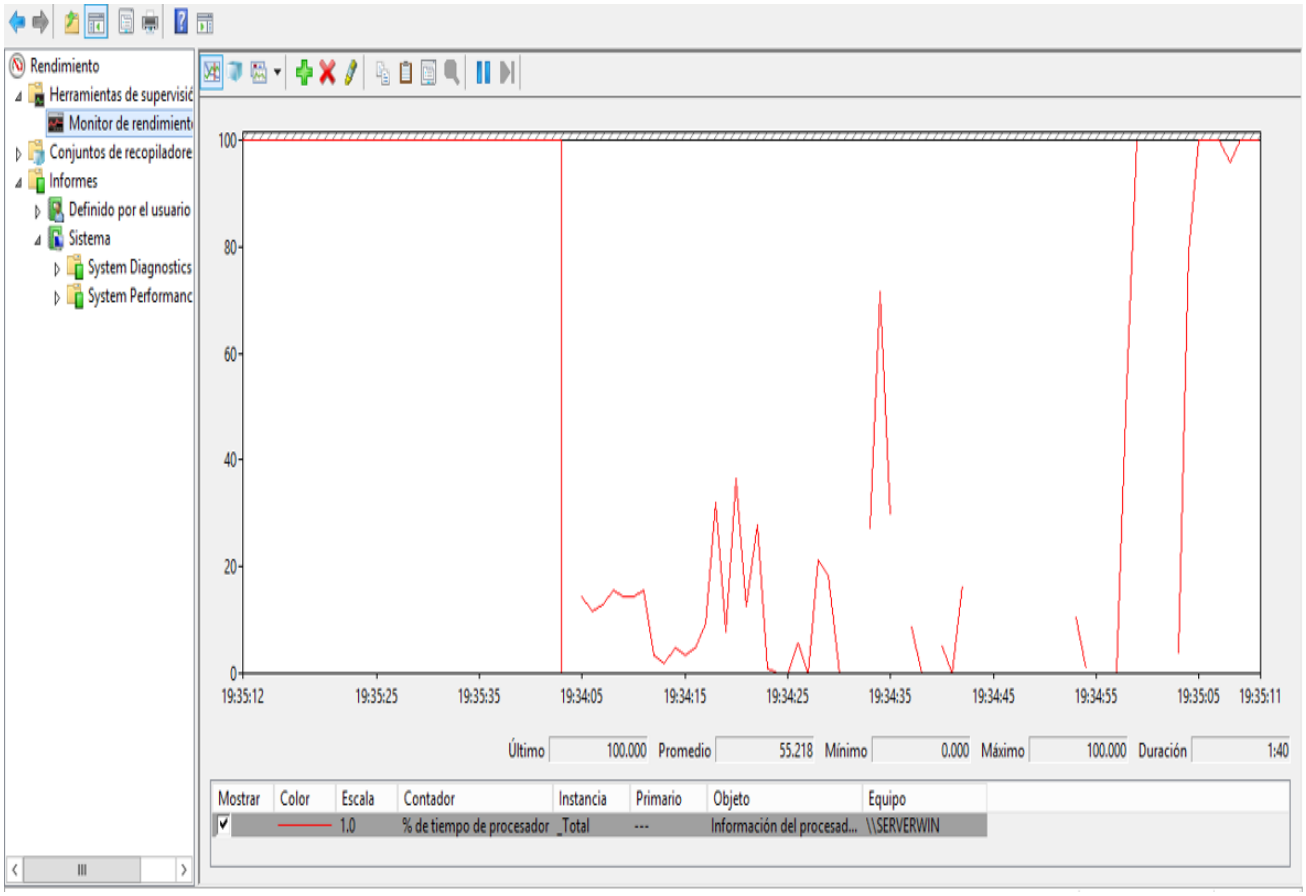

Figura 41: Rendimiento del Servidor Windows antes del ataque.
Fuente: Monitor Rendimiento Windows Server 2012

Figura 42: Rendimiento del Servidor Windows Ejecutando el ataque.
Fuente: Monitor Rendimiento Windows Server 2012

Explicación de la Figuras:

- El servidor de Windows (Windows Server 2012), se encuentra trabajando normalmente como se puede observar en la Figura 41 desde las 19:34.05.
- El ataque se realizó 19:35.05 por el cual el rendimiento del equipo subió considerablemente hasta saturar rendimiento de mi servidor por ende los servicios se saturaron y el servidor dejo de funcionar debido al ataque realizado.
- El ataque continuo hasta 19:36.25, en el cual se procedió a detenerlo como se observa en la Figura 42 y el rendimiento de mi servidor vuelve a funcionar con normalidad.

3.8.Cuarto ataque realizado al servidor Linux (Ubuntu 18.2) red WLAN con ip pública Servidor apache2 y Webmin.

3.8.1 Ataque Realizado al Servidor Apache2

El servidor ***apache2*** esta inicializado por el cual se comprobó mediante la dirección ip pública y el puerto activo.

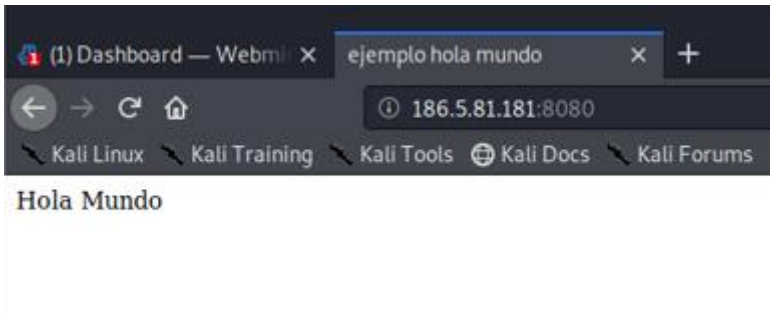

Figura 43: Verificación de Navegación de Servidor Apache2.
Fuente: Navegación ip pública Linux

Se procedió a realizar el ataque al servidor Ubuntu 18.04 servidor instalado es ***apache2*** mediante la Consola Metasploit de la herramienta Kali Linux.

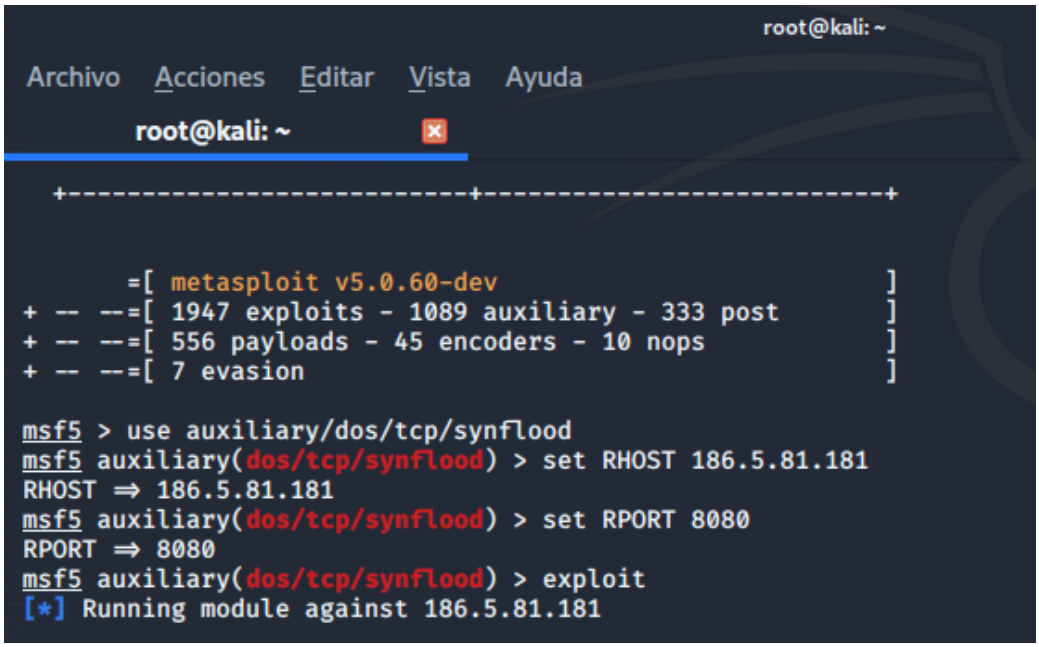

Figura 44: Ataque realizado al servidor Apache2 mediante Metasploit desde Kali Linux.
Fuente: msfConsole Kali Linux

Se verifica que los servicios de nuestra ip pública hayan caído navegando desde la ip pública y respectivo puerto.

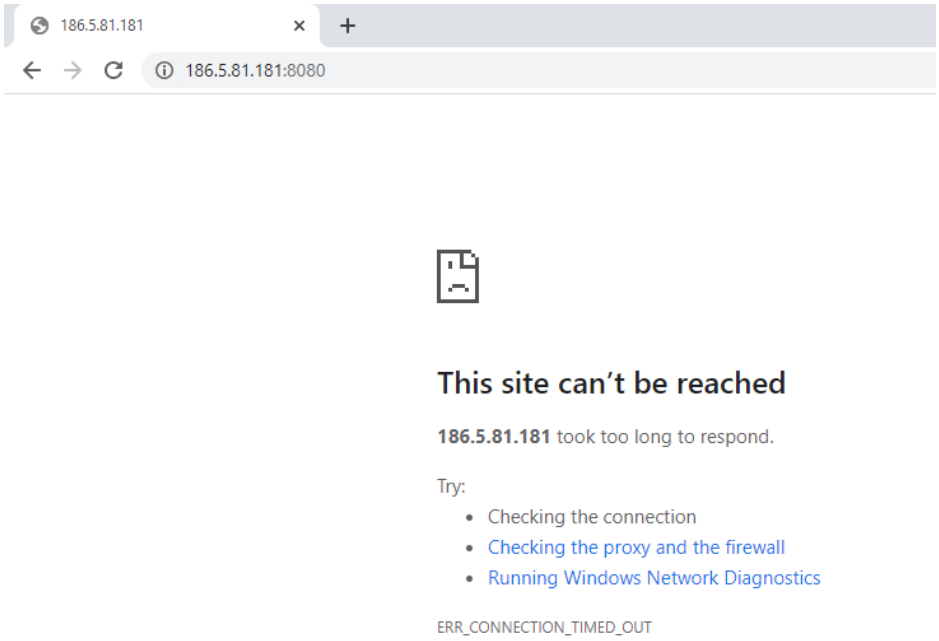

Figura 45: Verificación de la caída de Servicios del Servidor Apache2 Navegando desde la dirección ip Pública.
Fuente: Navegación ip publica Linux

Se detiene en lo posterior el ataque y se verifica que los servicios se vuelven a levantar del servidor web Linux Ubuntu 18.04 (apache2).

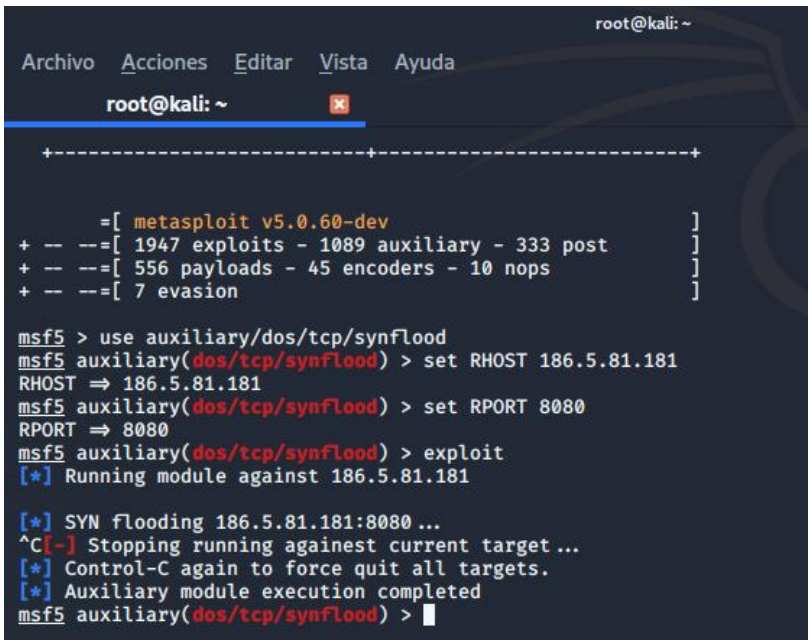

Figura 46: Detención del ataque al Servidor Apache2 mediante Metasploit.
Fuente: msfConsole Kali Linux

Se verifica que los servicios se hayan levantado nuevamente navegando en la dirección ip pública.

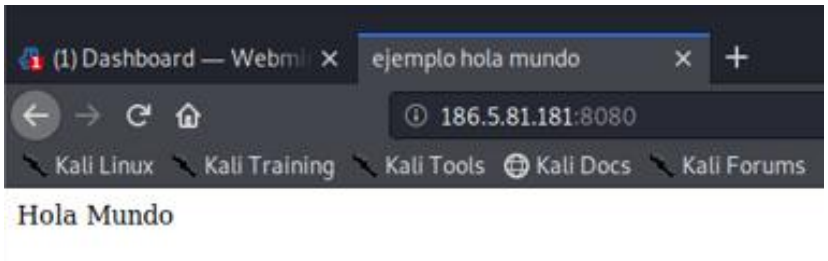

Figura 47: Verificación que los servicios este Levantado en el Servidor Apache2 navegando desde la dirección ip Pública.
Fuente: Navegación ip publica Linux

3.8.2 Ataque realizado Servidor Webmin

Ataque realizado a servidor Webmin con Metasploit desde Kali Linux utilizando una dirección ip pública y para este ataque se utilizó el puerto de Webmin puerto 10000

El servidor ***Webmin*** esta inicializado por el cual se comprobó mediante la dirección ip pública y el puerto activo.

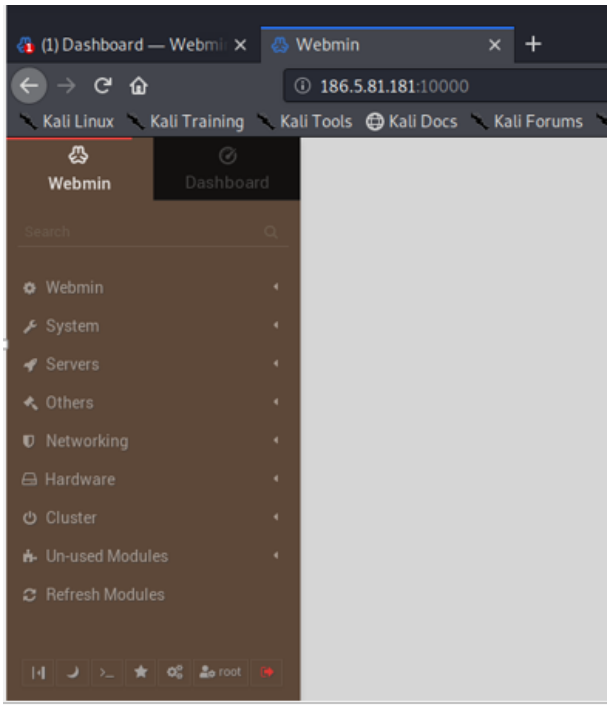

Figura 48: Verificación de que Servidor Web min este Navegando mediante la dirección ip pública y el puerto respectivo
Fuente: Imagen Webmin

Se procedió a realizar el ataque al Host Ubuntu 18.04 servidor instalado es ***Webmin*** mediante la Consola Metasploit de la herramienta Kali Linux.

Figura 49: Ataque realizado a servidor Webmin mediante Metasploit.
Fuente: msfConsole Kali Linux

Se verifica que los servicios de la ip pública hayan caído navegando desde la ip pública y respectivo puerto.

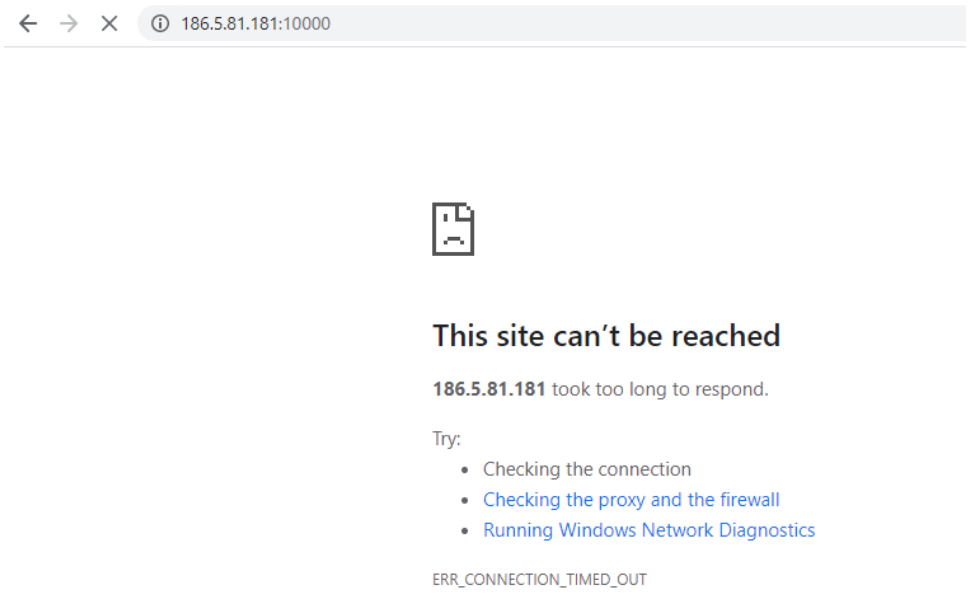

Figura 50: Verificación que los servicios de servidor Webmin hayan caído navegando en la dirección ip Pública.
Fuente: Navegación ip pública Webmin

Además, se puede observar al momento de realizar el ataque no solo cayeron los servicios del servidor públicamente de igual manera los servicios localmente ya que se intentó levantar manualmente los servicios el cual evito ingresar desde servidor Webmin como se puede observar en la figura 61.

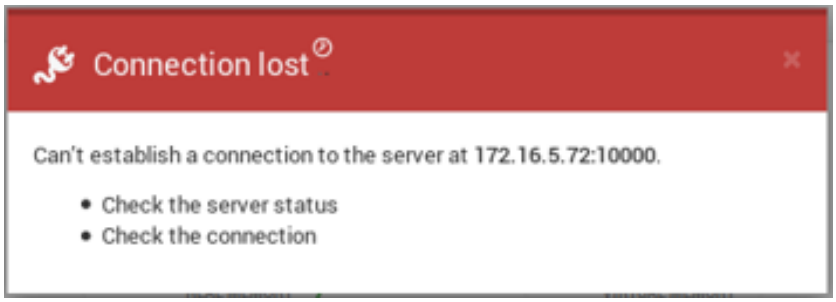

Figura 51: Verificación de los servicios Caídos en Servidor Webmin Localmente.
Fuente: Webmin

Se detiene en lo posterior el ataque y se verifica que los servicios se vuelven a levantar del servidor web Ubuntu 18.04 (Webmin)

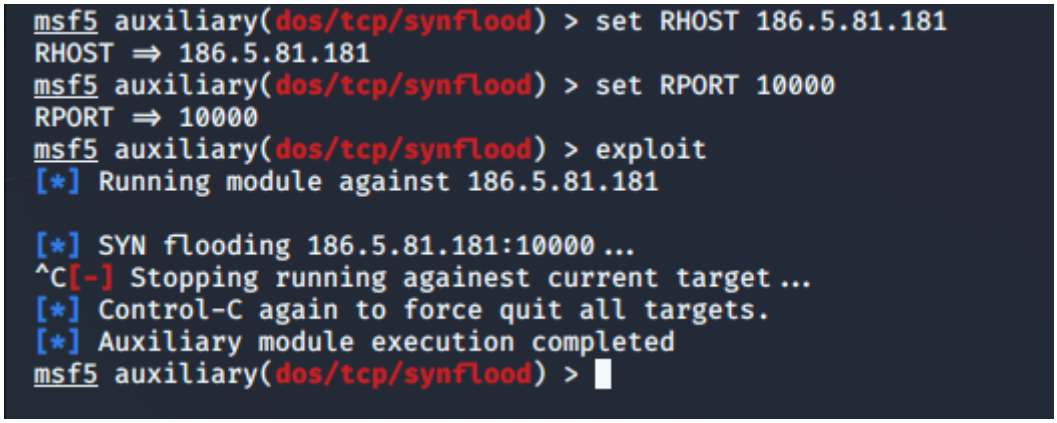

Figura 52: Detención del ataque realizado al Servidor Webmin Mediante Metasploit.
Fuente: msfConsole Kali Linux

Se verifica que los servicios se hayan levantado nuevamente navegando en la dirección ip pública del servidor web Webmin.

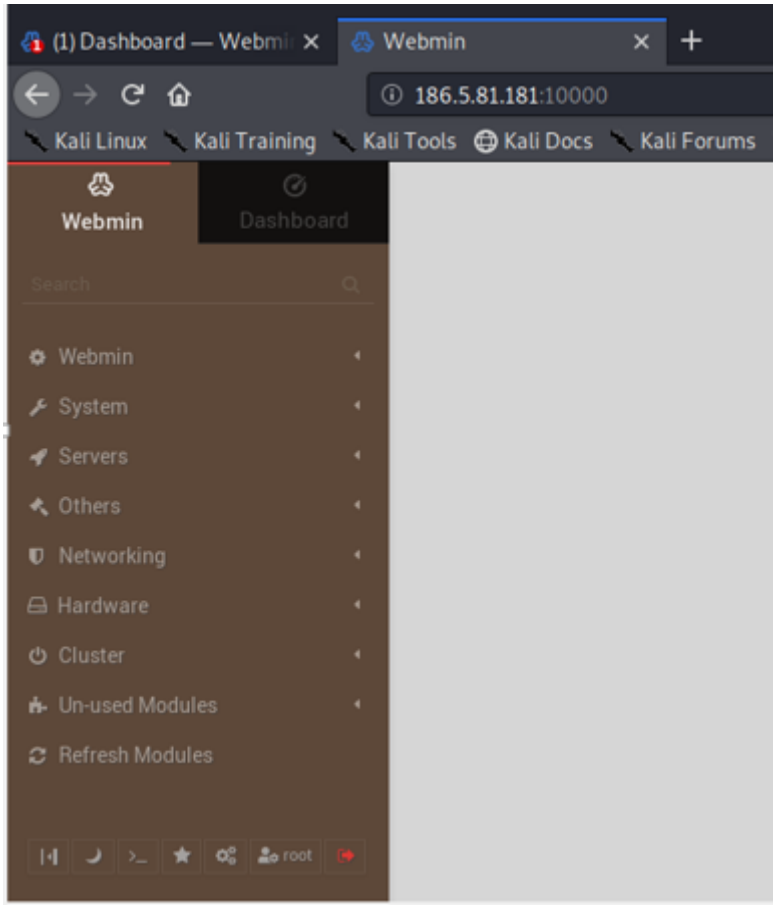

Figura 53: Verificación que los servicios del Servidor Webmin se hayan levantado nuevamente.
Fuente: Imagen Webmin

De igual manera que en el ataque anterior, se verifica cómo reacciona el servidor al momento de realizar el ataque monitoreando el servidor mediante el ***Monitor de Webmin*** que se encuentra en ***System Information*** del servidor Linux (Ubuntu 18.04) utilizando servidor ***Webmin*** obteniendo los siguientes resultados.

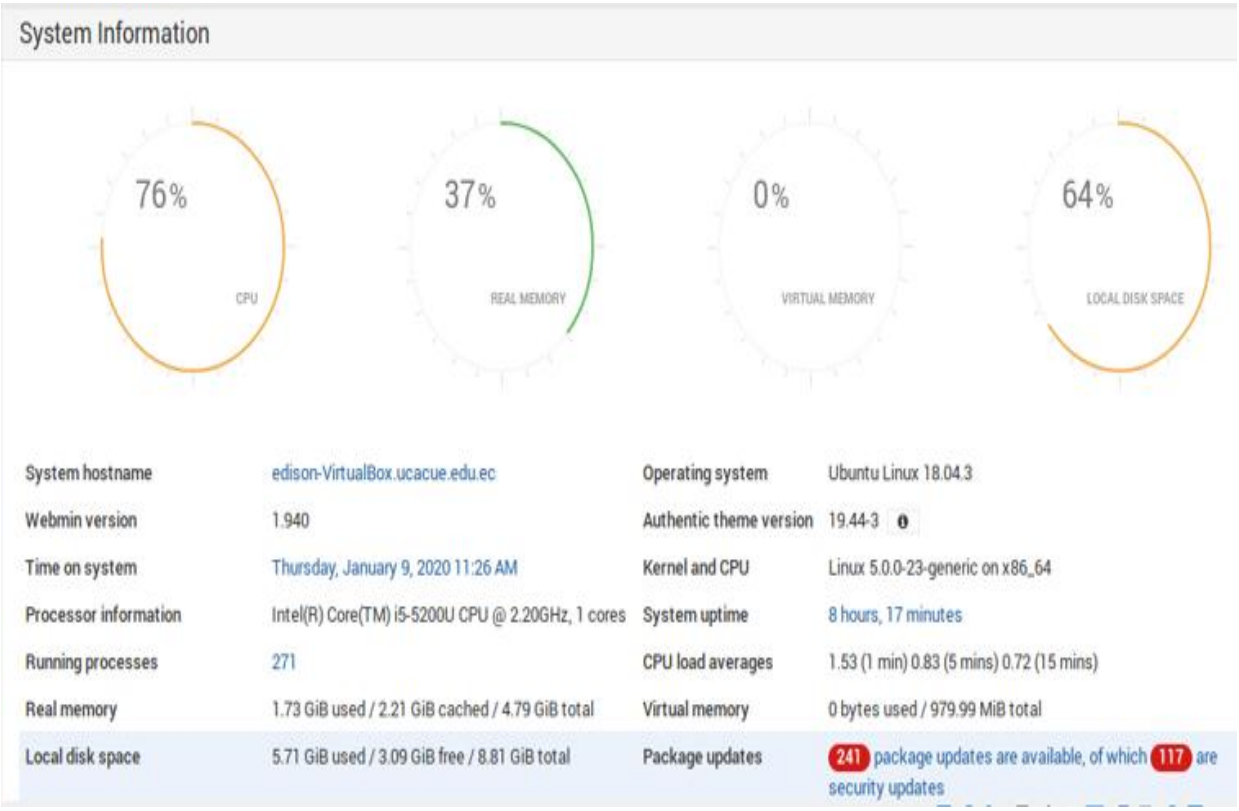

Figura 54: Rendimiento del Servidor Linux antes del ataque.
Fuente: System Information Webmin

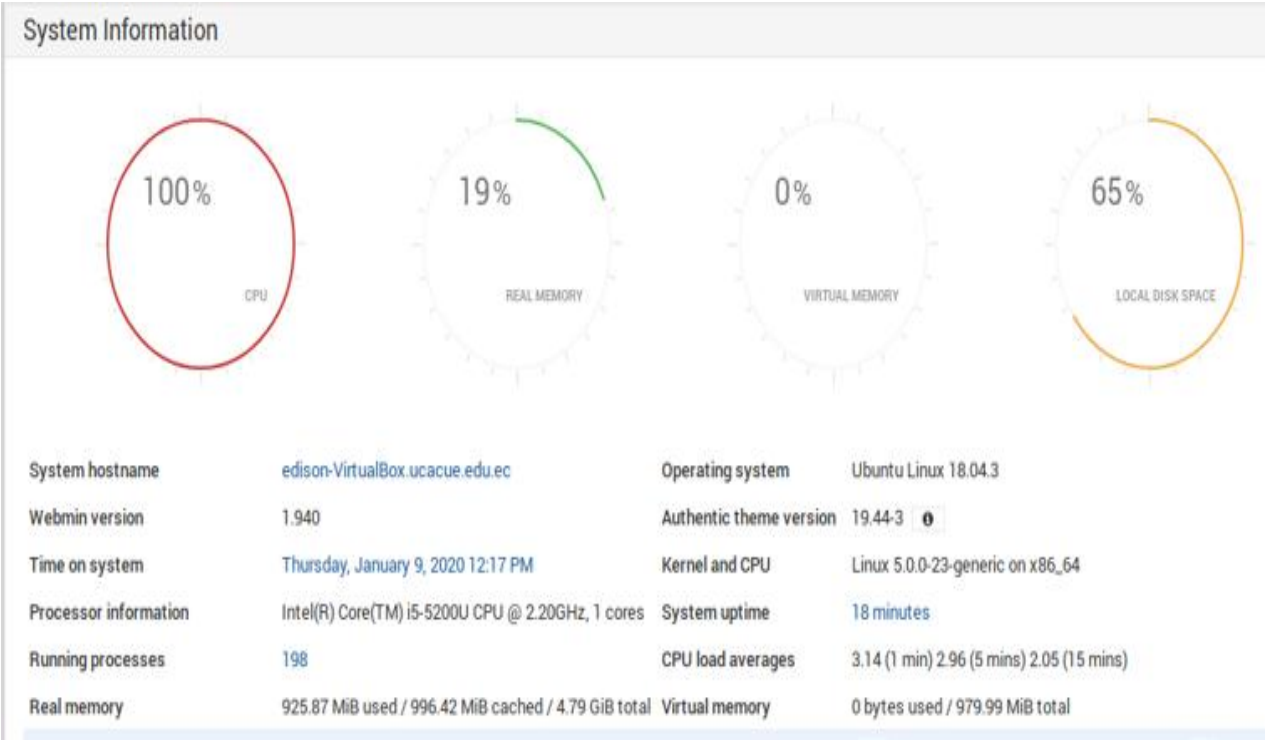

Figura 55: Rendimiento del Servidor Linux Ejecutando el ataque.
Fuente: System Information Webmin

Explicación de las Figuras:

a) El servidor de Linux Ubuntu 18.04 (Webmin), se encuentra trabajando normalmente como se puede observar en la figura 54.

b) Lugo de realizar el ataque al servidor subió considerablemente el rendimiento de la maquina como se observa en la figura 55 hasta saturar rendimiento del servidor por ende los servicios se saturaron y el servidor dejo de funcionar debido al ataque realizado.

c) Al finalizar el ataque del servidor volvió a funcionar con normalidad y se pudo observar que los servicios volvieron a inicializarse.

3.9 Leyes Vigentes en el Ecuador Contra Delitos Informáticos.

3.9.1 Breve Historia

Una de las primeras definiciones sobre los delitos informáticos se estableció en 1983, cuando la OCDE (Organización de Cooperación y Desarrollo Económico), definió como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos". (Verdezoto, 2020a)

En este caso "Troyano", fue el nombre del primer virus masivo reportado IBM PC en 1984, a raíz de esto, varios Estados de los E.E.U.U. fueron los primeros en contar con una ley específica para proteger los sistemas informáticos de las instituciones públicas. (Verdezoto, 2020b)

De esta manera el delito informático es un acto ilícito que se comete a través de herramientas informáticas, medios y dispositivos tecnológicos y de comunicación, con el objetivo de causar daño o provocar pérdidas de alguna índole o a su vez impedir el uso de algún sistema informático. (POLICIA NACIONAL DEL ECUADOR, 2017a)

Las actividades que contemplen, grabaciones y fotografías sin consentimiento o autorización legal, suplantación de claves electrónicas, daños o pérdida de información intencional, intervención o violación en la intimidad de las personas, entre otras, son ilícitas. (POLICIA NACIONAL DEL ECUADOR, 2017b)

3.9.2 Leyes Vigentes Contra delitos informáticos en el Ecuador.

En la actualidad, el Ecuador cuenta con Leyes que sancionan este tipo de delitos con penas de privación de libertad, los mismos que están reconocidos en el Código Orgánico Integral Penal (COIP), (Verdezoto, 2020c), entre ellos tenemos:

1. C.O.I.P. Art. 190.- Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. (Corte Nacional de Justicia, 2018a)
2. C.O.I.P. Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. (Corte Nacional de Justicia, 2018b)
3. C.O.I.P. Art. 195.- Infraestructura ilícita. - La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. (Corte Nacional de Justicia, 2018c)

4. C.O.I.P. Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. (Corte Nacional de Justicia, 2018d)

   Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. (Corte Nacional de Justicia, 2018e)

5. C.O.I.P. Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

   1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (Corte Nacional de Justicia, 2018f)

   2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de

tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. (Corte Nacional de Justicia, 2018g)

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. (Corte Nacional de Justicia, 2018h)

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (Corte Nacional de Justicia, 2018i)

6. C.O.I.P. Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. (Corte Nacional de Justicia, 2018j)

   Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (Corte Nacional de Justicia, 2018k)

7. C.O.I.P. Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos,

mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (Corte Nacional de Justicia, 2018l)

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. (Corte Nacional de Justicia, 2018m)

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (Corte Nacional de Justicia, 2018n)

8. C.O.I.P. Art. 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. (Corte Nacional de Justicia, 2018o)

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización

correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad. (Corte Nacional de Justicia, 2018p)

9. C.O.I.P. Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. - La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Corte Nacional de Justicia, 2018q)

4. Determinación de riesgos y vulnerabilidades, conclusiones y recomendaciones.

4.1. Análisis de los riesgos

Para analizar los riesgos de esta investigación se utilizó, MAGERIT versión 3.0 metodología de análisis y gestión de riesgos de los sistemas de información.

Introducción

La guía metodológica de MAGERIT. Se presume el conocimiento y comprensión de los conceptos de análisis y gestión de riesgos.

El objetivo es describir algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos. (Miguel Angel Amutio Gómez, 2012a)

Para cada una de las técnicas:

- Se explica brevemente el objetivo que se persigue al utilizarlas,
- Se describen los elementos básicos asociados,
- Se exponen los principios fundamentales de elaboración,
- Se presenta una notación textual y/o gráfica y
- Y se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia.

Todas las técnicas de esta metodología pueden utilizarse sin ayudas automatizadas; pero su aplicación repetitiva o compleja recomienda el empleo de herramientas tan amplia y frecuentemente como sea posible.

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la notación que desee, la que suele utilizar o la que ofrecen sus herramientas de desarrollo, respetando las

reglas y restricciones específicas de las distintas técnicas. (Miguel Angel Amutio Gómez, 2012b)

Técnicas específicas

Técnicas específicas de los proyectos de análisis y gestión de riesgos, técnicas que no se utilizan en otros contextos de trabajo.

Se han considerado de especial interés:

1. Uso de tablas para la obtención sencilla de resultados
2. Técnicas algorítmicas para la obtención de resultados elaborados
3. Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información

Para esta investigación se precede a utilizar la técnica de un **Análisis mediante tablas**

Análisis mediante tablas

Este análisis dice la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto. (Miguel Angel Amutio Gómez, 2012c)

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas. (Miguel Angel Amutio Gómez, 2012d)

Activos

Iniciando de manera conceptual “Se denominan Activos de Información a todos aquellos recursos de valor para una organización que generan, procesan, almacenan o transmiten información”. (Acosta, s.f.a)

La protección de los activos es esencial para la gestión de los riesgos ya que la no disponibilidad causaría un perjuicio o costes para la empresa. (Acosta, s.f.b)

Para el análisis de riesgos de esta investigación los activos son:

1. [S]Servidores
   - Windows Server 2012
   - Linux Ubuntu 18.04
2. [SW]Servicios Web
   - Navegador
   - Internet
   - Puertos
   - Direcciones Ip
   - Dominio
3. [SA]Servicios de aplicación
   - Local
   - Publico

Identificación de Riesgos, Vulnerabilidades y Amenazas

El objetivo de este paso es identificar los riesgos y vulnerabilidades de los activos ya mencionados anteriormente, y que fueron encontrados en el trabajo.

Riesgos

Se presenta a continuación una lista de los riesgos encontrados sobre los activos ya identificados:

Riesgos/Activos/Servidores/Servicios Web/Servicios de Aplicación

- Las configuraciones por defectos son vulneradas fácilmente
- Configuración por defecto del puerto web del servidor
- Limitación de recurrencia de peticiones
- Kali Linux es una herramienta de fácil uso que permite vulnerabilidad del firewall
- Caída de la red
- Caída de Servidores
- Inadecuado o no control de acceso.
- No disponibilidad de Servicio.

Vulnerabilidades

Se presenta a continuación una lista de vulnerabilidades encontrados sobre los activos ya identificados:

Vulnerabilidades/Activos/Servidores/Servicios Web/Servicios de Aplicación

- Falta de aplicativos para contrarrestar ataques como antivirus.
- Falta de implementación de políticas de seguridad
- Falta de implementación de políticas de firewall
- Falta Encriptación de puertos.

Amenazas

Se presenta a continuación una lista de Amenazas encontrados sobre los activos ya identificados en este caso de origen humano son causadas por acciones intencionales y de entorno que son provocados por interrupción prolongada de servicios electrónicos o de comunicaciones:

Amenazas/Activos/Servidores/Servicios Web/Servicios de Aplicación

- Hacheo realizado de fácil manera
- Posible utilización de sniffer para Crackeo de información
- Ausencia de operador de servidores
- Ataques mediante herramienta Kali Linux de hackeo

Tabla de Valoración de Riesgos/Vulnerabilidades/Amenazas

Matriz de la determinación de la probabilidad		
Impacto	**Probabilidad**	**Riesgo/Vulnerabilidad/ Amenazas**
MA: muy alto	MA: prácticamente seguro	**MA: critico**
A: alto	A: probable	**A: importante**
M: medio	M: posible	**M: apreciable**
B: bajo	B: poco probable	**B: bajo**
MB: muy bajo	MB: muy raro	**MB: despreciable**

Tabla 1 Valoración/vulnerabilidad/Amenazas

Fuente: (Miguel Angel Amutio Gómez, 2012)

Matriz de la determinación del impacto		
Criterio	**Impacto**	**Calificación**
Catastrófico	interrupción de 1hora	**5**
Significativo	Interrupción de 30 minutos	**4**
Moderado	interrupción de 15 minutos	**3**
Menor	interrupción de 10 minutos	**2**
Insignificante	interrupción menor a 1 minuto	**1**

Tabla 2 Determinación del Impacto

Fuente: (Miguel Angel Amutio Gómez, 2012)

Teniendo en cuenta las matrices se procede a calificar la probabilidad y el impacto los riesgos/vulnerabilidades /amenazas.

Riesgos			
Las configuraciones por defectos son vulneradas fácilmente			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*4*

Tabla 3 Riesgo las configuraciones por defectos son vulneradas fácilmente

Fuente: Elaboración del autor

Riesgos			
Configuración por defecto del puerto web del servidor			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*2*

Tabla 4 Riesgo configuración por defecto del puerto web del servidor
Fuente: Elaboración del autor

Riesgos			
Limitación de recurrencia de peticiones			
Probabilidad		***Impacto***	
Calificación:	*M*	*Calificación:*	*3*

Tabla 5 Riesgo limitación de recurrencia de peticiones
Fuente: Elaboración del autor

Riesgos			
Kali Linux es una herramienta de fácil uso que permite vulnerabilidad del firewall.			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*3*

Tabla 6 Riesgo Kali Linux es una herramienta de fácil uso que permite vulnerabilidad del firewall.
Fuente: Elaboración del autor

Riesgos			
Caída de la red			
Probabilidad		***Impacto***	
Calificación:	*B*	*Calificación:*	*1*

Tabla 7 Riesgo caída de la red
Fuente: Elaboración del autor

Riesgos			
Caída de Servidores			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*4*

Tabla 8 Riesgo caída de Servidores
Fuente: Elaboración del autor

Riesgos			
Inadecuado o no control de acceso.			
Probabilidad		***Impacto***	
Calificación:	*B*	*Calificación:*	*2*

Tabla 9 Riesgo inadecuado o no control de acceso.
Fuente: Elaboración del autor

Riesgos			
No disponibilidad de servicio			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*5*

Tabla 10 Riesgo no disponibilidad de servicio
Fuente: Elaboración del autor

Vulnerabilidad			
Falta de aplicativos para contrarrestar ataques como antivirus.			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*3*

Tabla 11 Vulnerabilidad falta de aplicativos para contrarrestar ataques como antivirus.
Fuente: Elaboración del autor

Vulnerabilidad			
Falta de implementación de políticas de seguridad			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*3*

Tabla 12 Vulnerabilidad falta de implementación de políticas de seguridad
Fuente: Elaboración del autor

Vulnerabilidad			
Falta de implementación de políticas de firewall			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*3*

Tabla 13 Vulnerabilidad falta de implementación de políticas de firewall
Fuente: Elaboración del autor

Vulnerabilidad			
Falta de encriptación de puertos			
Probabilidad		***Impacto***	
Calificación:	*MB*	*Calificación:*	*1*

Tabla 14 Vulnerabilidad falta de encriptación de puertos
Fuente: Elaboración del autor

Amenazas			
Hacheo realizado de fácil manera			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*4*

Tabla 15 Amenaza hacheo realizado de fácil manera
Fuente: Elaboración del autor

Amenazas			
Posible Utilización de sniffer para Crackeo de información			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*4*

Tabla 16 Amenaza posible Utilización de sniffer para Crackeo de información
Fuente: Elaboración del autor

Amenazas			
Ausencia de operador de servidores			
Probabilidad		***Impacto***	
Calificación:	*A*	*Calificación:*	*3*

Tabla 17 Amenaza ausencia de operador de servidores
Fuente: Elaboración del autor

Amenazas			
Ataques mediante herramienta Kali Linux de hackeo			
Probabilidad		***Impacto***	
Calificación:	*MA*	*Calificación:*	*5*

Tabla 18 Amenaza ataques mediante herramienta Kali Linux de hackeo
Fuente: Elaboración del autor

Graficas de estimación

Combinando probabilidad e impacto nos da la siguiente grafica según la valoración dada a los riesgos.

Leyenda de Grafica

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Tabla 19 Leyenda Grafica
Fuente: Elaboración del autor

Valoración

MATRIZ DE RIESGOS

RIESGO	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
• Las configuraciones por defectos son vulnerada fácilmente	5	4	20	Muy grave
• Configuración por defecto del puerto web del servidor	4	2	8	Apreciable
• Limitación de recurrencia de peticiones	3	3	9	Importante
• Kali Linux es una herramienta de fácil uso que permite vulnerabilidad los firewall	4	3	12	Importante
• Caida de la red	2	1	2	Marginal
• Caida de Servidores	5	4	20	Muy grave
• Inadecuado o no control de acceso.	2	2	4	Apreciable
• No disponibilidad de Servicio.	5	5	25	Muy grave

Tabla 20 Matriz de Riesgo
Fuente: Elaboración del autor

Resultados

RESULTADOS							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5				20	25
	ALTA	4		8	12		
	MEDIA	3			9		
	BAJA	2	2	4			
	MUY BAJA	1					

Tabla 21 Resultados Gravedad Impacto
Fuente: Elaboración del autor

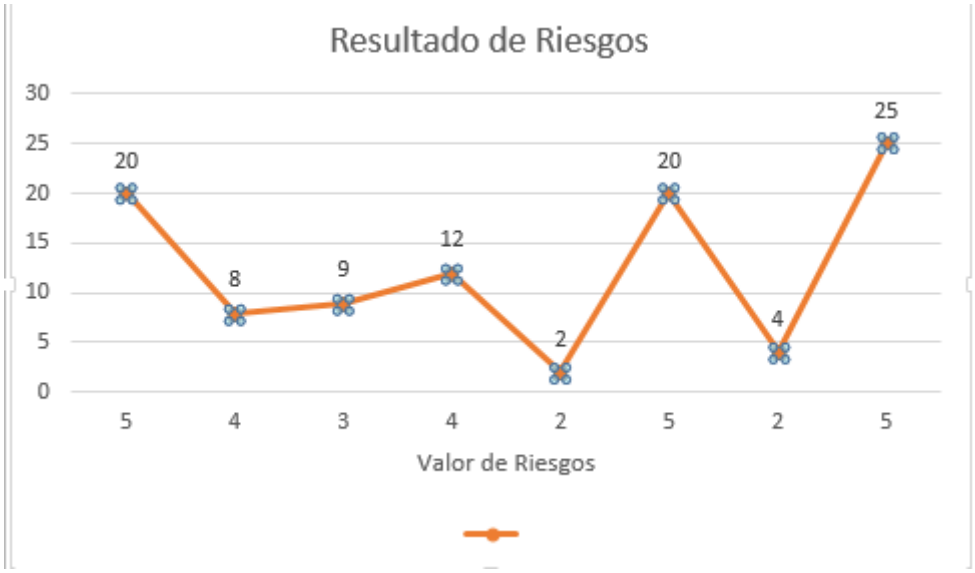

Figura 56 Resultado de Riesgos
Fuente: Elaboración del autor

Combinando probabilidad e impacto nos da la siguiente grafica según la valoración dada a las vulnerabilidades.

Leyenda de la grafica

	Vulnerabilidad muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Vulnerabilidad importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Vulnerabilidad apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Vulnerabilidad marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Tabla 22 Leyenda de la grafica
Fuente: Elaboración del autor

Valoración

MATRIZ DE VULNERABILIDAD

VULNERABILIDAD	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor de la vulnerabili	Nivel de la vulnerabilidad
• Falta de aplicativos para contrarrestar ataques como antivirus.	4	3	12	Importante
• Falta de implementación de politicas de seguridad	4	3	12	Importante
• Falta de implementación de politicas de firewall	4	3	12	Importante
• Falta Encriptación de puertos.	1	1	1	Marginal

Tabla 23 Matriz de Vulnerabilidad
Fuente: Elaboración del autor

Resultados

RESULTADOS							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5					
	ALTA	4			12		
	MEDIA	3					
	BAJA	2					
	MUY BAJA	1	1				

Tabla 24 Resultados de Vulnerabilidad
Fuente: Elaboración del autor

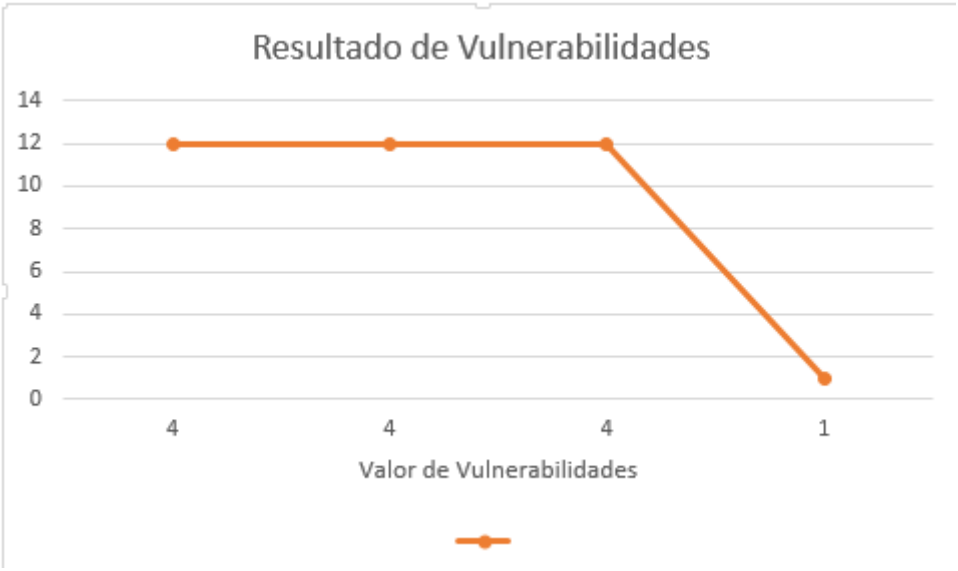

Figura 57 Resultado de Vulnerabilidad
Fuente: Elaboración del autor

Combinando probabilidad e impacto nos da la siguiente grafica según la valoración dada a las amenazas.

Leyenda de la grafica

	Amenaza muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Amenaza importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Amenaza apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Amenaza marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Tabla 25 Leyenda de la Grafica
Fuente: Elaboración del autor

Valoración

MATRIZ DE AMENAZAS

AMENAZAS	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor del la amenaza	Nivel de la amenaza
• Hacheo realizado de fácil manera	5	4	20	Muy grave
• Posible Utilización de sniffer para Crackeo de información	5	5	25	Muy grave
• Ausencia de operador de servidores	4	3	12	Importante
• Ataques mediante herramienta Kali Linux de hackeo	5	5	25	Muy grave

Tabla 26 Matriz de amenazas
Fuente: Elaboración del autor

Resultados

RESULTADOS							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5				20	25
	ALTA	4			12		
	MEDIA	3					
	BAJA	2					
	MUY BAJA	1					

Tabla 27 Resultados de Amenazas
Fuente: Elaboración del autor

Figura 58 Resultado de amenazas
Fuente: Elaboración del autor

Salvaguardas

Las salvaguardias son una medida para contrarrestar la presencia de un daño o posible daño a un determinado activo de la organización.

En la presente investigación se procederá a contrarrestar los daños Muy Graves.

Propuestas salvaguardas para contrarrestar este tipo de riesgos que tendrán los servidores.

Cambiar las configuraciones de firewall según normas o técnicas por ejemplo mejora continua.	
Descripción	Tipo
Las configuraciones por defecto son vulneradas de fácil manera.	[M] Minimización de Impacto de Riesgo [PR] Preventiva

Tabla 28 Salvaguardas según normas y técnicas
Fuente: Elaboración del autor

Proteger mediante Antivirus, Cortafuegos, Políticas de Firewall implementando los mismos.	
Descripción	Tipo
Se minimizaría el riesgo de la caída de los Servidores y por ende evitaría la no disponibilidad de los servicios.	[M] Minimización de Impacto de Riesgo [PR] Preventiva

Tabla 29 Salvaguardia de protección
Fuente: Elaboración del autor

Monitorización con personal capacitado.	
Descripción	Tipo
Evitar todo tipo de inconvenientes en servidores ataques, hackeos, perdida o divulgación de información etc.	[M] Minimización de Impacto de Riesgo [PR] Preventiva [AD]administrativa [CR] Correctiva

Tabla 30 Salvaguardia de Recursos Humanos
Fuente: Elaboración del autor

4.2.Conclusiones

Durante el desarrollo de la presente investigación evidenciamos que los ataques de Denegación de servicios, provocados y/o ocasionados por diferentes tipos de escenarios pueden llegar a tener efectos muy grandes para las organizaciones una de ellas la caída total del o los sistemas:

- Se demostró un alto grado de vulnerabilidad al no tener herramientas y políticas de seguridad correctas como por ejemplo objetivos de calidad o mejora continua, por lo tanto, Kali Linux vulneró con facilidad los servidores y sistemas operativos.

- Se pudo demostrar que, debido a configuraciones inadecuadas, el servicio web http es vulnerable en un 80 % con lo que expone elementos del servidor web a posibles ataques (DoS, rastreo de puertos). Las Configuraciones por defecto del firewall no impidió que el atacante no vulnere los servicios de los servidores.

- Diariamente se liberan nuevas amenazas y no siempre pueden estar embebidas en el software, sino también mediante ingeniería social, correo electrónico y páginas web.

- La base teórica fue muy importante y sirvió como un manual para poder aplicar los diferentes tipos de ataques a los servicios.

- Con el resultado de análisis planteado sobre el funcionamiento de herramientas para hackeo podemos observar que existen diferentes vulnerabilidades en este caso referidos a los servidores web.

- Al analizar y manipular las herramientas de hackeo, se comprobó y mejoro toda la información y conocimiento acerca de ataques a servidores web, también observamos cómo estos afectan a los servicios tanto de hardware como software de los servidores en línea.

- El mayor riesgo encontrado fue directamente en los servicios que fueron detenidos, es decir todos recursos, procesos y tareas, ya no estuvieron disponibles.

- Se pudo observar que los riesgos son altamente peligrosos para la información de los servidores ya que las políticas de seguridad no pudieron detectar los ataques realizados.

- El ataque DoS provoco un riesgo de alto impacto, afectando la credibilidad de los servidores, a esto podemos agregar una pérdida económica muy grande.

    - Se demostró un alto grado de riesgo 100% en riesgo de “no disponibilidad de servicio” al no tener acceso a los servidores según análisis de riesgos.

4.3.Recomendaciones

Podemos nombrar las siguientes recomendaciones, que pueden ser tomadas en cuenta a corto o largo plazo, dependiendo de las necesidades de acuerdo a cada organización.

- Contar con un licenciamiento de antivirus siempre actualizado que nos permita controlar cualquier tipo de software malicioso o ataque que intente vulnerar a los servicios web.

- Mantener siempre los navegadores actualizados, algunos parches de actualización incluyen módulos de seguridad para evitar que atacantes puedan acceder al historial de navegación.

- Crear políticas en el firewall con los permisos necesarios para los servidores web.

- Complementar con un sistema para detección de intrusos en modo de ataque.

- Constantes mantenimientos en las diferentes configuraciones de los servidores web para evitar los ataques de denegación de servicios y otros.

- Contar con personal debidamente capacitado en el área de seguridad de la información para contrarrestar estos incidentes.

- Monitorizar el mayor tiempo posible los diferentes recursos de los servidores como son CPU, Memoria RAM, Almacenamiento de esta manera se puede estar alerta a un posible ataque.

- La seguridad de la información depende siempre de la correcta administración y funcionamiento del firewall, el cual debe ser monitoreado por personal

capacitado el mismo que notificara ante cualquier intento de ataque a los directivos de las organizaciones.

BIBLIOGRAFÍA

Acaparros. (2016, Abril 19). *Escuela de organizacion industrial*. Retrieved from Ciberseguridad: https://www.eoi.es/blogs/ciberseguridad/2016/04/19/el-caso-ronnie-ataque-dos-denegacion-de-servicio-distribuidos/

Acosta, F. (n.d.). *Material adicional del Seminario Taller Riesgo vs. Seguridad de la Información*. Retrieved from https://www.academia.edu/14050403/Material_adicional_del_Seminario_Taller_Riesgo_vs._Seguridad_de_la_Informaci%C3%B3n

Aguilar, P. C. (2007, Febrero). *Administración de redes*. Retrieved from https://www.monografias.com/trabajos43/administracion-redes/administracion-redes2.shtml

Alvarez, G. V. (n.d.). *"SEGURIDAD EN REDES IP: DOS/DDOS".* Retrieved from https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf

Alvarez, J. K. (2013, junio). *Manual de Wireshark*. Retrieved from http://manualwiresharkjeny.blogspot.com/2013/06/11-caracteristicas-de-wireshark_17.html

Anrrango, R. (2014, Septiembre 30). *Conceptos Generales de WINBOX*. Retrieved from Conceptos Generales de WINBOX: https://configurarmikrotikwireless.com/blog/conceptos-winbox-configurar-mikrotik.html

Azamar, A. (2017, 11 11). *Electrónica y seguridad informática*. Retrieved from Electrónica y seguridad informática: https://securityassessmentsblog.wordpress.com/2017/11/11/ataque-dns-spoofing/

Bruno Chavarria Neira, E. G. (2017). *IMPLEMENTACIÓN DE UN SERVIDOR WEB Y UN DISEÑO DE UNA PÁGINA UTILIZANDO HERRAMIENTAS DE SOFTWARE LIBRE PARA EL DISPENSARIO "SAGRADA FAMILIA"DE LA CIUDAD DE GUAYAQUIL.* Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/14162/1/GT001840.pdf

Bueno, A. (2012, MArzo 13). *Redes informaticas*. Retrieved from Tecnología: https://www.buenastareas.com/ensayos/Redes-Informaticas/3664047.html

Catoira, F. (2012, Marzo 28). *Consejos para evitar un ataque de denegación de servicio*. Retrieved from https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

Corte Nacional de Justicia. (2018, Febrero 05). *CODIGO ORGANICO INTEGRAL PENAL, COIP*. Retrieved from CODIGO ORGANICO INTEGRAL PENAL, COIP: https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

Cruz Saavedra, W. G. (2014, junio 02). *Universidad privada del norte*. Retrieved from Aplicación de auditoría penetration testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo: http://repositorio.upn.edu.pe/handle/11537/10239?show=full

Desdelinux. (n.d.). *Webmin: Administración desde el navegador web*. Retrieved from https://blog.desdelinux.net/webmin-administracion-desde-el-navegador-web/#comments

DigitalOcean. (2016, Marzo 23). Retrieved from https://blog.digitalocean.com/update-on-the-march-24-2016-dns-outage/

Fernandez, E. E. (2010, Junio). *Virtualización de servidores de telefonía IP en GNU/Linux.* . Retrieved from http://www.adminso.es/recursos/Proyectos/PFC/PFC_eugenio.pdf

Gaibor, A. V. (2007, Octubre). *Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones.* . Retrieved from https://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

Garcia, M. S. (2006). *¿Qué es un servidor y cuáles son los principales tipos de servidores? (proxy, dns, web, ftp, smtp, etc.).* Retrieved from https://www.aprenderaprogramar.com/attachments/article/542/DV00408A%20Que%20es%20un%20servidor%20principales%20tipos%20proxy%20smtp%20ftp%20web%20dns.pdf

Gonzalez, G. (2018, Marzo 14). *Genbeta*. Retrieved from Ataque : https://www.genbeta.com/actualidad/github-acaba-de-sobrevivir-el-ataque-ddos-mas-grande-de-la-historia

Gutierrez, R. P. (2013, Julio 01). *Clase practica seguridad escaneo con nma* . Retrieved from https://es.slideshare.net/RobertPuicanGutierrez/clase-practica-seguridad-escaneo-con-nma-pf-23733850

Jeria, M. (2016). *Los ataques de DoS.* Retrieved from https://repositorio.espe.edu.ec/bitstream/21000/11609/2/T-ESPE-053040-R.pdf

Leandres, A. M. (2019, Julio 2019). *Construcción de un modelo de red virtual para aplicar técnicas de hacking ético y poder analizar los eventos relacionados a la seguridad informática sobre una infraestructura virtual.* Retrieved from http://repositorio.unajma.edu.pe/bitstream/handle/123456789/489/Alex_Tesis_Bachiller_2019.pdf?sequence=1&isAllowed=y

Lee, D. (2013, Marzo 27). *Global internet slows after 'biggest attack in history'*. Retrieved from Technology reporter, BBC News: https://www.bbc.com/news/technology-21954636

Lois, A. (2012, Mayo 14). *Ataques "Man in the middle [MITM]" (ARP Spoofing/Poisoning) sobre IPv4. 2012.* . Retrieved from https://www.zonasystem.com/2012/05/ataques-man-in-middle-mitm-arp.html

Luis, V. R. (2014). *instalacion y configuracion del software de servidor web*. Retrieved from https://books.google.com.ec/books?id=RrfbCgAAQBAJ&pg=PT105&lpg=PT105&dq=est%C3%A1+dise%C3%B1ado+para+transferir+hipertextos,+p%C3%A1ginas+web+y+paginas+HTML+(Hypertext+Markup+Language);+generalmente+funciona+a+trav%C3%A9s+del+puerto+80&source=bl&ots=R9qkN

Masgnulinux. (2018, Fefrero 08). *¿Qué es Kali GNU/Linux?* Retrieved from https://maslinux.es/que-es-kali-gnu-linux/

Mejia, G. E. (2018). *ESTUDIO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE VIRTUALIZACIÓN DE SERVIDORES DE APLICACIONES PARA LA CARRERA DE LICENCIATURA DE SISTEMAS DE INFORMACIÓN*. Retrieved from http://repositorio.ug.edu.ec/bitstream/redug/37044/1/TESIS%20GUALBERTO%20MORETTA-FINAL.pdf

MetaSploit. (2011, marzo 11). *Comandos y Conceptos Básicos MetaSploit Framework*. Retrieved from https://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/

Miguel Angel Amutio Gómez, J. C. (2012, Octubre). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* . Retrieved from https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

NEXTVISION. (2018, 05 29). *Tag Archives: ataques*. Retrieved from Tag Archives: ataques: https://www.nextvision.com/tag/ataques/

Osabuena. (2015, Enero 05). *Ataques Port Scanner o Escaneo de Puertos*. Retrieved from https://osabuena.com/seguridad-informatica/ataques-port-scanner-o-escaneo-de-puertos

POLICIA NACIONAL DEL ECUADOR. (2017, Diciembre 27). *Delitos informáticos establecidos en el COIP y como prevenirlos*. Retrieved from Delitos informáticos establecidos en el COIP y como prevenirlos: https://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Posada, O. O. (2013, Noviembre 08). *Tecnología de información.* . Retrieved from ¿ Que es y como instalar metasploit en Ubuntu ?: https://oscaromarposadasanchez.blogspot.com/2013/11/

Rodriguez, D. (2019). *lifender.com*. Retrieved from Investigación aplicada: características, definición, ejemplos: https://www.lifeder.com/investigacion-aplicada/

Romero, J. L. (2014). *Instalacion y configuracion del software de servidor web*. Retrieved from https://books.google.com.ec/books?id=RrfbCgAAQBAJ&pg=PT105&lpg=PT105&dq=est%C3%A1+dise%C3%B1ado+para+transferir+hipertextos,+p%C3%A1ginas+web+y+paginas+HTML+(Hypertext+Markup+Language);+generalmente+funciona+a+trav%C3%A9s+del+puerto+80&source=bl&ots=R9qkN

Saltos, C. A. (2017, Agosto). *ESTRATEGIA DE HACKING ÉTICO Y LOS NIVELES DE SEGURIDAD EN LA INTRANET DE LA COOPERATIVA DE AHORRO Y CRÉDITO 13 DE ABRIL LTDA DE LA CIUDAD DE "VENTANAS"* . Retrieved from http://dspace.uniandes.edu.ec/bitstream/123456789/8426/1/TUBMIE008-2017.pdf

Sanchez, J. A. (2013, Mayo). *DISEÑO Y CONSTRUCCIÓN DE UNA RED IP VIRTUALIZADA PARA LA APLICACIÓN DE HACKING ÉTICO*. Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/4908/6/UPS%20-%20ST000994.pdf

Sanchez, O. O. (2013, Noviembre 08). *Tecnología de información*. Retrieved from ¿ Que es y como instalar metasploit en Ubuntu ?: https://oscaromarposadasanchez.blogspot.com/2013/11/

Sensors tech forum. (2017, Julio 14). *kali linux*. Retrieved from https://sensorstechforum.com/es/kali-linux-what-you-need-know/

Serra Ruiz J, R. L. (2009, Septiembre). *Análisis forense de sistemas informáticos*. Retrieved from https://es.scribd.com/document/218828626/Analisis-forense

Significados. (2018, Septiembre 06). *Tecnologia e Innovación* . Retrieved from https://www.significados.com/hacker/

Tori, C. (2008, Mayo). *Hacking Etico*. Retrieved from https://es.slideshare.net/WaldirNuezFrancia1/hacking-etico-carlos-tori-52185274

Ulloa, L. F. (2009, Enero 15). *LA VIRTUALIZACIÓN Y SU IMPACTO EN LAS CIENCIAS COMPUTACIONALES*. Retrieved from https://www.funlam.edu.co/revistas/index.php/lampsakos/article/view/779/748

Velazquez, E. (2009, Enero 08). *Pymes y Autonomos*. Retrieved from ¿Qué es la virtualización? : https://www.pymesyautonomos.com/tecnologia/que-es-la-virtualizacion

Velez, I. S. (2006). *Las redes informaticas*. Retrieved from https://scholar.google.com/scholar?hl=es&uact=5&um=1&ie=UTF-8&lr&q=related:cSo08NzfjBsUHM:scholar.google.com/l

Verdezoto, J. M. (2020). *DERECHOECUADOR*. Retrieved from DELITOS INFORMÁTICOS O CIBERDELITOS: https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos

ANEXOS

TESIS Edison González V.1

INFORME DE ORIGINALIDAD

6%	5%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www1.monografias.com Fuente de Internet	<1%
2	www.recercat.cat Fuente de Internet	<1%
3	infoleg.mecon.gov.ar Fuente de Internet	<1%
4	luismmm.blogspot.com Fuente de Internet	<1%
5	estudiobandin.blogspot.com.ar Fuente de Internet	<1%
6	osabuena.com Fuente de Internet	<1%
7	cabinasylocutorios.blogspot.com Fuente de Internet	<1%
8	Submitted to Universidad de Valladolid Trabajo del estudiante	<1%
9	Submitted to University of Applied Sciences	<1%

	Berlin Trabajo del estudiante	
10	Submitted to Uniagustiniana Trabajo del estudiante	<1 %
11	funlam.edu.co Fuente de Internet	<1 %
12	www.usm.edu.ec Fuente de Internet	<1 %
13	Submitted to Universidad Andina del Cusco Trabajo del estudiante	<1 %
14	Submitted to Universidad de Nebrija Trabajo del estudiante	<1 %
15	www.computerworld.es Fuente de Internet	<1 %
16	www.cejamericas.org Fuente de Internet	<1 %
17	www.argenval.com.ar Fuente de Internet	<1 %
18	bdigital.unal.edu.co Fuente de Internet	<1 %
19	www.upv.cz Fuente de Internet	<1 %
20	alerta-antivirus.red.es Fuente de Internet	<1 %

21	informatica-juridica.com Fuente de Internet	<1%
22	repositorio.upct.es Fuente de Internet	<1%
23	www.aciprensa.com Fuente de Internet	<1%
24	www.solomanuales.org Fuente de Internet	<1%
25	ceraelyse.blogspot.com Fuente de Internet	<1%
26	www.ictp.csic.es Fuente de Internet	<1%
27	www.aprenderaprogramar.com Fuente de Internet	<1%
28	193.87.16.4 Fuente de Internet	<1%
29	www.planetalinux.com.ar Fuente de Internet	<1%
30	www.intelexport.com Fuente de Internet	<1%
31	www.noticias.com Fuente de Internet	<1%
32	www.gte.us.es Fuente de Internet	<1%

33	foro.adsib.gov.bo Fuente de Internet	<1%
34	www.linguee.com Fuente de Internet	<1%
35	Submitted to SUNY, Binghamton Trabajo del estudiante	<1%
36	Submitted to Universitat Politècnica de València Trabajo del estudiante	<1%
37	matrix.it.uc3m.es Fuente de Internet	<1%
38	www.3com.com Fuente de Internet	<1%
39	windowsxp.datafull.com Fuente de Internet	<1%
40	support.microsoluciones.net Fuente de Internet	<1%
41	howtoscomos.blogspot.com Fuente de Internet	<1%
42	www.usoli.org Fuente de Internet	<1%
43	madrid.sindominio.net Fuente de Internet	<1%
44	Submitted to Universidad Pontificia Bolivariana	

	Trabajo del estudiante	<1%
45	Submitted to Olathe South High School Trabajo del estudiante	<1%
46	mafiadoc.com Fuente de Internet	<1%
47	Daniel Mellado. "", IEEE Latin America Transactions, 7/2007 Publicación	<1%
48	oa.upm.es Fuente de Internet	<1%
49	Submitted to University of Edinburgh Trabajo del estudiante	<1%
50	"New Advances in Information Systems and Technologies", Springer Science and Business Media LLC, 2016 Publicación	<1%

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Activo		

PERMISO DEL AUTOR DE TESIS PARA SUBIR AL REPOSITORIO INSTITUCIONAL

Yo, EDISON GIOVANNY GONZALEZ GONZALEZ, portador (a) de la cédula de ciudadanía Nro. 0302302062. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"ANÁLISIS DE DENEGACIÓN DE SERVICIOS EN SERVIDORES WEB, WINDOWS Y LINUX"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de Los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, Así mismo; autorizo a la Universidad para que realice la publicación de éste trabajo de titulación en Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, 09 de marzo de 2020

F: .....

EDISON GIOVANNY GONZALEZ GONZALEZ

0302302062

Universidad Católica de Cuenca

EL BIBLIOTECARIO DE LA SEDE AZOGUES

Que: **GONZÁLEZ GONZÁLEZ EDISON GIOVANNY**, con cédula de ciudadanía Nro. **0302302062** de la Carrera de **Ingeniería en Sistemas.**

No adeuda libros, a esta fecha: **10 de marzo de 2020**

Eco. Fabián Rodríguez Herrera
BIBLIOTECARIO

Biblioteca Universitaria
MONS. "EROILAN POZO QUEVEDO"

CENTRO DE IDIOMAS

ABSTRACT

Author: Edison González González
Tutor: Ing. Miguel Andrade López

The main objective of this research work is the analysis and simulation of Denial of Service (DoS) attacks on Windows and Linux Web Servers.

For this, the Windows Server 2012 operating system was used in Windows and for Linux Ubuntu Server 18.04.

The research covers highlights on the application of Open Source tools such as: Virtual BOX, Kali Linux to demonstrate vulnerabilities on servers in both Windows and Linux.

It started with an introduction to data networks, servers and web services, in which fundamental network concepts are reviewed, and all those aspects involved in a network and the internet and this paper in particular.Subsequently, the Denial of Service (DoS) attacks were presented, and a brief review of them and the tools to perform the attack.

Finally, it was shown the Analytical and Explanatory section, where a Denial of Services (DoS) attack on WEB Servers was simulated, to understand how an attacked system behaves and how the Services are affected, using the tools mentioned, to provide responses on how to counteract this type of attack, with the recommendation of applications, firewalls, patches which would avoid the materialization of the threats detected.

KEYWORDS: SERVERS, NETWORKS, DOS, ATTACKS, COMMUNICATIONS.

Azogues, 11 de marzo del 2020

EL CENTRO DE IDIOMAS DE LA UNIVERSIDAD CATÓLICA DE CUENCA, CERTIFICA QUE EL DOCUMENTO QUE ANTECEDE FUE TRADUCIDO POR PERSONAL DEL CENTRO PARA LO CUAL DOY FE Y SUSCRIBO

Abg. Liliana Urgilés Amoroso, Esp.
COORDINADORA CENTRO DE IDIOMAS AZOGUES