UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

CREACIÓN DE UN PLAN DE CONTINGENCIA QUE DISMINUYA LOS ATAQUES A WEB SITES MEDIANTE LA DETECCIÓN DE ANOMALÍAS

MORENO GARINO PATRICIO STEFANO
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

CREACIÓN DE UN PLAN DE CONTINGENCIA QUE DISMINUYA LOS ATAQUES A WEB SITES MEDIANTE LA DETECCIÓN DE ANOMALÍAS

MORENO GARINO PATRICIO STEFANO
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

CREACIÓN DE UN PLAN DE CONTINGENCIA QUE DISMINUYA LOS ATAQUES A WEB SITES MEDIANTE LA DETECCIÓN DE ANOMALÍAS

MORENO GARINO PATRICIO STEFANO
INGENIERO DE SISTEMAS

CARTUCHE CALVA JOFFRE JEORWIN

MACHALA, 27 DE SEPTIEMBRE DE 2022

MACHALA
2022

tesis

INFORME DE ORIGINALIDAD

5%	5%	0%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	maestriainformaticamg.blogspot.com Fuente de Internet	1%
2	dspace.utb.edu.ec Fuente de Internet	1%
3	Submitted to Universidad de Málaga - Tii Trabajo del estudiante	<1%
4	riul.unanleon.edu.ni:8080 Fuente de Internet	<1%
5	repositorio.utmachala.edu.ec Fuente de Internet	<1%
6	openwebinars.net Fuente de Internet	<1%
7	docplayer.net Fuente de Internet	<1%
8	melinafernandezln.blogspot.com Fuente de Internet	<1%
9	repositorio.uandina.edu.pe Fuente de Internet	<1%

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, MORENO GARINO PATRICIO STEFANO, en calidad de autor del siguiente trabajo escrito titulado CREACIÓN DE UN PLAN DE CONTINGENCIA QUE DISMINUYA LOS ATAQUES A WEB SITES MEDIANTE LA DETECCIÓN DE ANOMALÍAS, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 27 de septiembre de 2022

MORENO GARINO PATRICIO STEFANO
0704988120

DEDICATORIA

El presente trabajo va dedicado primeramente a mi madre, quien cada día me incentivó a seguir adelante y poder llegar hasta donde he llegado ahora, inculcándome valores que me sirven en el día a día para ser mejor persona.

De igual manera, a todas las personas que me dieron el impulso de seguir y no abandonar la etapa de estudios para poder conseguir mi título universitario.

Patricio Stefano Moreno Garino

AGRADECIMIENTO

Primeramente, doy las gracias a la Universidad por ayudarme a seguir mi formación académica, brindarme la oportunidad de no desistir de mis estudios y así de poder lograr un objetivo más.

También a los docentes que compartieron un poco de sus conocimientos y experiencias que ayudaron a formarme como profesional, para llegar a este momento de la culminación de la etapa más la vida estudiantil.

Finalmente, agradezco a mi familia, amigos y familiares cercanos, quienes con sus alientos y buenas energías me ayudaron en esta ocasión a poder terminar este trabajo, logrando así estar más cerca de obtener el título universitario

Patricio Stefano Moreno Garino

RESUMEN

Actualmente, la mayoría de web sites optan por mejorar su seguridad al ver todo lo que puede suceder si no se tiene los debidos controles, un sitio web no seguro genera muy mala reputación para quien lo haya realizado y a su vez genera desconfianza para los demás usuarios que vayan a usarlo. Motivo por el cual se puede llegar a ser víctima de robo de información alojada en estos. Con el robo de información pueden surgir muchos problemas tanto para la empresa que administra la página web afectada como para el usuario final. Este último es el afectado en cierta forma dado a que puede llegar a ser víctima de un delito informático dándose un posible caso de extorsión o alguno otro problema grave de esta calamidad. También muchas de las veces por desconocimiento se tratan de corregir rápidamente los errores sin tener en cuenta que la solución que se está aplicando, posiblemente no sea la correcta, llevando a agravar el problema existente creando brechas difíciles de detectar y, en muchos de los casos, corregir a tiempo.

Esto puede llegar a desembocar un efecto negativo a gran escala si es que esto no se lo logra controlar a tiempo. Así mismo como existe el robo de información, existe otras maneras de perjudicar un servicio web, en donde estos pueden negarse a dar acceso a ellos, es decir, mediante el hallazgo de brechas de seguridad se logran infiltrar para poder causar una negación parcial o total de una acción con diferentes modos y herramientas. Dicho de otra manera, la denegación de servicio produce una falta de disponibilidad de un recurso determinado, dado sea el ejemplo de acceder a correo electrónico, conectividad o de algún otro servicio. En casos más extremos, millones de personas podrían verse obligadas temporalmente a dejar de usar el recurso que está siendo intervenido por personas que originan el ataque. En otros casos, los delincuentes también utilizan este método para dañar programas y archivos en los sistemas informáticos.

Dado al creciente desarrollo tecnológico, las personas que se dedican a actos delictivos informáticos optan por ir mejorando sus métodos de vulnerar sus objetivos, creando metodologías o scripts novedosos que permitan lograr su meta la cual es causar daño a sus víctimas en la mayoría de casos. Teniendo en cuenta esto, las formas de proteger la información almacenada y todo lo que pueda ser afectado por estas personas y sus métodos más recientes, es también ir desarrollando nuevas formas para poder llegar a evitar o prevenir en un futuro posibles robos, ataques, sustracción, perdida de información y denegación del servicio usado.

Tratar de hacer una aplicación que sea 100% libre de fallos y vulnerabilidades no va a ser posible, pero si se puede planificar medidas de mitigación que permitan tomar acciones rápidas con el fin de no afectar el servicio al usuario. Es por ello que se propone analizar los posibles fallos y vulnerabilidades que pueden suscitarse al momento de navegar por un sitio web de manera normal, esto se lo hace con el objetivo de recolectar pruebas que permitan obtener resultados que ayuden formar un plan de contingencia en caso de que el web site o servidor usado, sea víctima de un hackeo.

Palabras clave: sitio web, fallos, vulnerabilidades, seguridad, información.

ABSTRACT

Currently, most web sites choose to improve their security by seeing everything that can happen if the proper controls are not in place, an unsafe website generates a very bad reputation for whoever has made it and in turn generates distrust for other users. that they are going to use it. Reason for which you can become a victim of theft of information hosted on them. With the theft of information, many problems can arise both for the company that manages the affected website and for the end user. The latter is affected in a certain way given that they can become the victim of a computer crime, giving rise to a possible case of extortion or some other serious problem of this calamity. Many times, due to ignorance, they try to quickly correct errors without taking into account that the solution being applied may not be the correct one, leading to aggravate the existing problem, creating gaps that are difficult to detect and correct in time in many of the case.

This can lead to a large-scale negative effect if this is not controlled in time. Just as there is information theft, there are other ways to harm a web service, where they can refuse to give access to them, that is, by finding security gaps they manage to infiltrate to cause a partial or total denial. of an action with different modes and tools. Put another way, denial of service results in a lack of availability of a given resource, for example access to email, connectivity, or some other service. In more extreme cases, millions of people could be temporarily forced to stop using the resource that is being seized by the originators of the attack. In other cases, criminals also use this method to damage programs and files on computer systems.

Given the growing technological development, people who engage in computer criminal acts choose to improve their methods of violating their objectives, creating novel methodologies or scripts that allow them to achieve their goal, which is to cause harm to their victims in most cases. Taking this into account, the ways to protect the stored information and everything that can be affected by these people and their most recent methods, is also to develop new ways to be able to avoid or prevent possible thefts, attacks, theft in the future, loss of information and denial of the service used.

Trying to make an application that is 100% free of bugs and vulnerabilities is not going to be possible, but it is possible to plan mitigation measures that allow quick actions to be taken in order not to affect the service to the user. That is why it is proposed to analyze the possible failures and vulnerabilities that can arise when browsing a website normally, this is done with the aim of collecting evidence that allows obtaining results that help form a contingency plan in case that the web site or server used is the victim of a hack.

Keywords: website, bugs, vulnerabilities, security, information.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

En estos tiempos, la tecnología en general para el uso de internet a ido creciendo y con ello la seguridad que conlleva. En los webs sites uno de los factores importantes, es la seguridad que pueda brindar cuando esta se esté usando, ya sea para diferentes aplicaciones u ocupaciones. Dado a este incremento tecnológico la seguridad se ve también afectada, a tal punto que nos podemos cuestionar si el sitio en el que estamos es seguro aun aplicando protocolos para prevenir colapsos o caídas. Si hablamos de seguridad informática, las personas encargadas de esta, deben estar preparados para los distintos escenarios en cuanto a salvaguardar la integridad, confidencialidad, usabilidad, etc, de la información almacenada. Por más que queramos proteger un sitio web, no habrá un 100% de éxito en este sentido, esto provoca que se genere vulnerabilidades y fallos en el transcurso del uso de internet.

Estos fallos o vulnerabilidades pueden ser aprovechados por personas maliciosas que desean quebrantar la seguridad del sitio web para acceder al contenido que tiene y ocuparlo para propósitos ilícitos. Mitigar estos tipos de fallos y brechas de seguridad son un poco complicadas si es que no se tiene el contexto indicado ni la información sobre las mismas, para ellos es más factible primero identificarlas antes de lanzarse a resolverlas, dado a que la solución que lleguen a implementar no necesariamente llegue a cubrir toda la problemática. A veces la falta de conocimiento respecto a la temática de seguridad y las amenazas que abundan actualmente alrededor de las aplicaciones conectadas a internet, puede resultar en un efecto negativo a gran escala, es decir, al no tener la noción de que es lo que puede afectar a una aplicación se puede llegar a caer en el error de que el sistema usado esta perfecto, no necesita mejora e inclusive llegar a pensar que está libre de todo mal que lo puede llegar a rodear.

Es necesario someter a las páginas web y a las aplicaciones en general a varias pruebas, con la intención de identificar todos fallos posibles los cuales puedan ser aprovechados por gente con malas intenciones y con ello poder dificultarles sus objetivos. Para esto existen personas enfocadas en este tipo de trabajos o evaluaciones las cuales permiten tener un panorama más amplio de las deficiencias de las aplicaciones que se usan y a su vez brindan informes de todo lo encontrado en las pruebas que se realizan. La seguridad de la información abarca varios aspectos de los cuales destacan lo informático, físico, telecomunicaciones, entre otros más.

Al tener la información resultante de las evaluaciones realizadas por este tipo de personas, lo que resta es implementar medias que permitan limitar y controlar en gran medida todo lo que se encontró en dichas evaluaciones, es decir, poner en marcha metodologías, modelos, técnicas, etc, que ayuden a reducir al mínimo los problemas encontrados y así con esto poder elevar significativamente la confiabilidad de estos sistemas con acceso a internet.

El presente documento se encuentra estructurado de la siguiente manera:

Capítulo I: Describe lo referente a la problemática existente, especificando requerimientos y dando su debida justificación con el fin de satisfacer la temática planteada con las necesitades encontradas en la misma.

Capítulo II: Se lleva a cabo la fundamentación teórica con bases bibliografías, planteamiento de objetivos y desarrollo de la investigación con el fin de obtener resultados favorables según lo previsto.

Capítulo III: Por último, se realiza la evaluación del escenario desarrollado para poder emitir las conclusiones y recomendaciones optimas en base a los objetivos que ayuden a resolver la temática planteada.

1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. ÁMBITO DE APLICACIÓN: DESCRIPCIÓN DEL CONTEXTO Y HECHOS DE INTERÉS

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades de los sistemas informáticos alojados en la web. Estos nuevos métodos de ataque se han ido mejorando, por lo que en muchos casos solo se necesitan conocimientos técnicos básicos para ejecutarlos. Cualquier usuario con una conexión a internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

Cuando el usuario entra a un sitio web y establece conexión con el sitio, este envía una petición al servidor en donde se encuentra alojado dado como resultado un ACK. Esto puede dar apertura a que se puedan enviar varias peticiones al servidor desde direcciones IP's desconocidas, logrando así una inestabilidad en la cola de solicitudes y por ende el colapso de este al no poder procesar todas las peticiones entrantes. Al darse el colapso, el servidor se cae dejando en su cola de peticiones, varias solicitudes pendientes. "Los equipos vulnerables a los ataques SYN dejan las conexiones abiertas en cola en una estructura de memoria de datos y aguardan la recepción de un paquete ACK." [1]

Los ataques SYN cada año se incrementan en cierto porcentaje. Esto es un gran problema que abarca a la mayoría de páginas web ya que no tienen los controles de seguridad debidos. "El atacante explota una debilidad conocida en la secuencia de conexión TCP" [2] dando a entender que, se envía muchas peticiones syn al servidor con la intención de poder saturar los recursos de la víctima.

En los últimos años, la empresa Eset mediante su reporte sobre la ciberseguridad, da a conocer datos acerca de ataques cibernéticos, [3] expresando que la gran mayoría las empresas asociadas a este reporte, afirman que la mayor amenaza que atraviesan en los ataques de este estilo son de tipo inyección de código malicioso, seguidas de robo y suplantación de información, entre otros más.

1.2. ESTABLECIMIENTO DE REQUERIMIENTOS A SATISFACER

La seguridad informática, en estos tiempos no es algo con lo que se deba de relajarse de cara a la protección de los datos recolectados y almacenados en web sites usados por el usuario común. Tomando en cuenta la situación por la que atraviesa el mundo, el uso de tecnologías que nos faciliten la productividad en nuestros trabajos y actividades cotidianas que impliquen una conexión de internet de por medio, se volvió algo normal y en ocasiones algo necesario. Pero esto también trae consigo consecuencias al estarlas usando, dado a que estas trabajan con información delicada del usuario, datos de la empresa y otras más.

Según la autora [4] de la web El País, expresa que “Las organizaciones necesitan operaciones de seguridad que puedan funcionar a la velocidad de la máquina para mantenerse al día con el volumen, la sofisticación y el ritmo de las ciber amenazas actuales” esto sin mencionar que el aumento en la criminalidad cibernética es evidente. Por ello, es de carácter obligatorio implementar contramedidas efectivas y eficientes para escenarios de este estilo, logrando así dificultar el trabajo a los hackers en cuanto a obtener información importante.

1.3. JUSTIFICACIÓN DE REQUERIMIENTO

Debido al creciente desarrollo de tecnologías y herramientas para el uso de internet, los ataques de personas con malas intenciones que cometen crímenes informáticos han evolucionado de manera preocupante, esto lo hacen para que sea más difícil ser encontrados cometiendo ciberdelitos y a su vez lograr su objetivo que es perjudicar los usuarios envueltos.

En los sitios web, la seguridad es algo primordial, dado al hecho de que los usuarios acceden brindan mucha información valiosa. No existe una web que este exenta de algún fallo o que tenga una seguridad indestructible, mientras más evolucione la tecnología y las formas de perpetuar la seguridad de una web, el incremento de vulnerabilidades y amenazas también aumentan.

Dentro de este contexto, la planificación de medidas preventivas y de mitigación para las amenazas de este estilo no se lo puede tomar a la ligera, ya que causan un efecto negativo hacia la seguridad informática y de los webs sites que alojan la información.

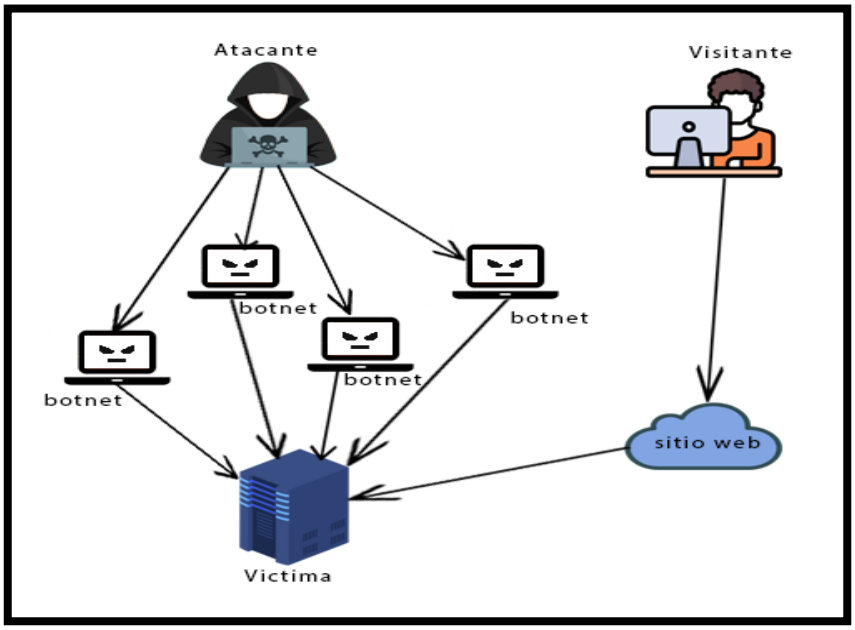
2. CAPÍTULO II. DESARROLLO DEL PROTOTIPO

2.1. DEFINICIÓN DEL PROTOTIPO TECNOLÓGICO

El escenario presente de esta simulación es de un sitio web el cual será sometido a ataques Dos con la intención de sacar fallos en la seguridad y a su vez desarrollar contramedidas que puedan mitigar los ataques realizados y evitar por su puesto que el sitio atacado no se vea afectado ante un ataque en ejecución.

La siguiente ilustración demuestra como sucede un ataque a un sitio web.

Ilustración 1: Ataque a un Web Site



Fuente: Elaboración propia.

2.2. FUNDAMENTACIÓN TEÓRICA DEL PROTOTIPO

Actualmente la pandemia generada por el virus Covid-19 ha causado que se cambie el estilo de vida de la población drásticamente, adoptando y reforzando métodos para actividades cotidianas que permitan culminar con éxito las mismas. Para ello el avance de tecnologías que se ven implicadas en cualquiera de las actividades avanza con el fin de aumentar la productividad y la comodidad.

Esto también trae consigo el aumento de fallos y vulnerabilidades en dichas tecnologías, por ejemplo, el uso de aplicaciones móviles y web, que llevan consigo información valiosa de la empresa o usuario, con ello la forma de robar información alojada en estas tecnologías también ha ido mejorando. Según [5] hace referencia sobre la ciberseguridad vista como un juego competitivo, en el que el atacante aprovecha las fallas del defensor para jugarlas en su contra, en cambio, el defensor hace todo lo que está a su alcance para impedir que el atacante logre su meta.

La concientización sobre los riesgos existentes en el internet, debe ser un factor primordial hacia las personas que usan este medio para manipular información. [6] Ninguna persona o empresa que administre aplicaciones web busca poner en riesgo toda la información que un usuario haya proporcionado, por ello estos administradores deben tener medidas preventivas, planes de contingencia que permitan tomar acciones rápidas para evitar algún ataque que desee atentar con la integridad informática de estas.

2.2.1. Espionaje Informático y Hacking

Normalmente el concepto de espionaje y hackeo informático van de la mano, incluso se relacionan en cierta forma. “El hacking se identifica con el acceso indebido a (datos de) sistemas informáticos”. [7] En ambos casos, el fin de realizar estos ciberdelitos es para conseguir información, datos de seguridad y daño de los sistemas vulnerados.

Según [8] argumenta que los hackers novatos tratan de meterse a grupos de este estilo tomando en cuenta que en dichos grupos existen gente que es consciente sobre sus actos respecto a lo que están haciendo, dependiendo el punto de vista en que se lo vea, la mayoría de veces se lo cataloga como algo indebido e ilícito, pero no todo es así, también se lo puede hacer para evaluar un software con la intención de elevar su protección y confiabilidad.

Con el tiempo, se ha logrado disminuir los ataques a sistemas conectados a la web gracias a la creación de artículos y sanciones referentes a estos tipos de delitos. Actualmente, la tendencia de ciberataques se ha reactivado nuevamente, dado a que el uso de aplicaciones e internet aumento por la crisis mundial que se atraviesa.

2.2.2. Ataque Informático

Los ataques informáticos fueron surgiendo a medida que los sistemas web fueron usados con más frecuencia, para esto, la seguridad de estos sistemas también tuvo que ir en aumento, ya que un ataque de este tipo nunca viene con buenas intenciones. En términos simples, “consiste en afectar cualquier recurso de información sobre una persona u organización.” [9] esto se lo hace para causar un efecto negativo en la seguridad del sistema, creando así brechas que permiten el acceso a delincuentes cibernéticos.

En definitiva, pensar en una contramedida que permita controlar en su gran mayoría estos fallos de seguridad siempre será bienvenido de parte de la empresa o de la persona que este a cargo, logrando así que los atacantes la tengan más difícil al tratar de hacer algo indebido en contra de estos.

2.2.3. Vulnerabilidad

Como se sabe, en cuestión de desarrollo de aplicaciones y sistemas, nunca por nunca se podrá desarrollar algo libre de fallos. Se conoce como vulnerabilidad al resultado de bugs en el diseño del sistema o de limitaciones tecnológicas. [10] También es considerada debilidad existente de un sistema que puede ser explotada por una persona mal intencionada, cuyo objetivo solo puede ser causar un impacto negativo hacia lo desarrollado, quebrantar su seguridad y extraer lo que necesita esa persona

2.2.4. Ataque Dos

Los ataques Dos (denials of services) pueden llegar a ocasionar sinnúmero de pérdidas a nivel empresarial si es que no se lo controla a tiempo. Como su nombre lo indica, el objetivo de este ataque es el de denegar el acceso a un servicio en concreto, [11] mandando muchas peticiones desde una maquina en particular, como por ejemplo ingreso a un sitio web de uso cotidiano con información bancaria o personal, o también el ingreso y uso de una aplicación móvil que tenga acceso a internet que maneje la información antes mencionada. [12]

2.2.5. Ataque DDos

A diferencia de los ataques Dos (denegación de servicios), este tipo de ataques recurre al manejo de grupos de ordenadores infectados. De igual manera con este tipo de ataques se desea negar el uso del servicio ya sea de forma parcial o total en la aplicación web de destino. [13]

2.2.6. Ataques de Phishing

Es un tipo de ataque de fraude electrónico, inicialmente es enviado un correo electrónico al usuario o grupo de usuarios víctima con nombres de empresas o instituciones de alto reconocimiento, todo eso para que se revele información confidencial. [14] Si se realiza con éxito y la persona o grupo de personas victimas caen en esto, se verán envueltas en un grupo de personas con identidades robadas, es decir, toman toda la información proporcionada por ellos para proceder a suplantar su identidad en diferentes tipos de actividades posibles.

2.2.7. Tipos de Ataques DDos

2.2.7.1. HTTP Flood (Saturación HTTP)

Entre muchos tipos de ciberataques aparece el http flood, el cual es un tipo de ataque volumétrico que aprovecha solicitudes GET o POST en los webs sites para atacar de forma maliciosa al servidor. “El enfoque principal de un ataque DDos de inundación HTTP es generar tráfico de ataque que simule de cerca la legitimidad de un usuario humano”. [15] Este tipo de ataques es el más habitual dado a que lleva a usar todos los recursos asignados del servidor en la aplicación atacada. [16]

2.2.7.2. SYN Flood

Este ataque como algunos otros más, intenta explotar un protocolo de internet. [17] Al ser bastantes peticiones que el servidor gestiona y da acceso, el tope de peticiones de clientes, se va llenando y esto trae como consecuencia que colapse al tratar de recibir una nueva conexión entrante de un nuevo usuario real. Existen mecanismos Anti-DDos, [18] los cuales permiten controlar en cierta manera el ataque, identificando parámetros que sirvan de entrenamiento a los mecanismos usados para automatizarlos.

2.2.7.3. Ping of Death (Ping de la Muerte)

Es un tipo de ataque Dos, el cual envía paquetes mediante la herramienta ping. [19] Normalmente al hacer una petición, esta tiene un tamaño de 32 bytes, pero con este tipo de ataque se puede aumentar el tamaño del paquete enviado, causando así problemas en la gestión y envió de las peticiones a los servidores.

2.2.7.4. Inyecciones SQL

En la negación de servicios, una inyección SQL puede realizar varias acciones, pero esto depende del objetivo del atacante. [20] Comúnmente lo que se hace es implantar una parte de código a nivel de base de datos, esto se hace para incrustar sentencias maliciosas de manera que faciliten el robo de credenciales y descargar malwares a los dispositivos que originan el acceso a la página infectada.

2.2.7.5. Inyección de Código

Este tipo de método como su nombre lo indica se basa en inyectar partes de un código previamente programado, con la intención de alterar el original y así poder acceder al contenido del sistema web afectado. [21] Este método es muy usado para obtener información de la persona que usa la aplicación y en su mayoría de veces es muy complicada su detección.

2.2.8. Web Application Firewall (WAP)

Como su nombre lo dice, es usado para proteger el acceso a una aplicación o servicio web, su seguridad está basado en modelos que implementan políticas ya sean estas positivas o negativas [22] es decir, puede permitir o denegar el tráfico de internet. Dependiendo de la modalidad en la que se lo emplee [23], los recursos y tiempos de respuesta serán de distintas cantidades, todo eso con el fin de disminuir significativamente la posibilidad de un ataque al servidor o a la aplicación.

2.2.9. Metodologías de Desarrollo

2.2.9.1. Cyber Kill Chain

Es parte del modelo Intelligence Drive Defense, se basa en la identificación y prevención de actividades intrusivas cibernéticas. [24] Es decir, identifica lo que el hacker necesita completar para lograr su objetivo y mediante una serie de pasos ayudan al analista a comprender la situación que está sucediendo. Se debe de completar un conjunto de actividades en combinación con grupos lógicos ejecutados en un orden correcto para poder crear el proceso de ataque con una duración definida. [25]

2.2.10. Estándares de Seguridad

2.2.10.1. ISO/IEC 27001

“Esta norma adopta un enfoque de proceso para establecer, implementar, operar, monitorear, evaluar, mantener y mejorar la seguridad de la información” [26] basándose en la planificación, implantación, verificación y control del sistema de gestión de seguridad de la información de una empresa. Tanto los controles para una evaluación de riesgo de la NESA como de la ISO/IEC 27001 son parecidos dado a que identifican el contexto para luego escoger criterios de riesgo y metodologías a aplicar. [27]

2.2.11. Plan de contingencia

Es de vital importancia desarrollar una contramedida que permita actuar ante alguna amenaza que se presente, este caso, crear un plan de contingencia que esté preparado para ser desplegado en caso de algún incidente es lo primero que se debe pensar en cuando una aplicación ya esté preparada para poner en funcionamiento. [28]

En pocas palabras, “el plan de contingencia describe como se debe actuar ante eventos que produzcan riesgos de continuidad en el negocio” [29] Una vez que se haya diseñado el plan debe ser sometido a pruebas las cuales serán con el propósito de verificar que la solución es óptima y en caso de existir punto débiles se deberá ajustarlos para una mayor eficiencia. El plan de contingencia está constituido por 8 fases las cuales:

2.2.11.1. Fase 1: Planificación

2.2.11.1.1. Diagnóstico

Si de seguridad informática se trata, el responsable de la misma debe estar preparado para diferentes escenarios, garantizando la integridad, confidencialidad, disponibilidad, etc. de la información almacenada. Por mucho que nos gustaría asegurar un sitio web, no será 100% exitoso en este sentido, lo que resultará en brechas y fallas en el uso de Internet. Comúnmente la carencia de controles en cuanto a la determinación de una cantidad limitada de conexiones entrantes a una página o al servidor web es una de las vulnerabilidades con mayor presencia, a su vez que, al conectarse desde dispositivos de procedencia desconocida, se puede llegar a pensar que traen consigo algún tipo de malware y esto puede llegar a afectar al destinatario, es decir, a la página que solicita la conexión.

Las personas malintencionadas pueden explotar estas fallas o vulnerabilidades para comprometer la seguridad de este sitio web para acceder al contenido que posee y utilizarlo con fines ilegales. Mitigar este tipo de fallas y vulnerabilidades de seguridad puede ser un poco complicado sin un contexto específico o información sobre las mismas, para ellos es más factible identificarlas primero antes de iniciar con su solución, ya que las soluciones que se pueden llegar a implementar no necesariamente abarcan con todo la problemática.

2.2.11.1.2. Organización Estructural

En la **Ilustración *2*** se puede visualizar como está constituido el escenario planteado en esta investigación.

2.2.11.1.3. Inventario de Recursos Informáticos

Los recursos informáticos utilizados son los siguientes:

- VMware Workstation
- Sistema operativo Kali Linux
- Sistema operativo Windows
- Fail2ban

2.2.11.1.4. Planificación (Establecimiento)

Se establecen los alcances del Plan de Contingencias, se procede con el levantamiento de herramientas de control que tienen la función de controlar y limitar las solicitudes de los protocolos de internet icmp, tcp y http, usados en las páginas web o servidores, ya que los mismos dan cabida a ataques que aprovechan estas vulnerabilidades tales como:

- Saturación o inundación http.
- Alto consumo de recursos físicos.
- Alto consumo de ancho de banda.

En el apartado de **Solución de la problemática** se especifica medidas de mitigación a seguir para solucionar los problemas presentados anteriormente.

2.2.11.2. Fase 2: Identificación de Riesgos

Para proceder de manera correcta se definen las limitaciones del alcance, según el orden establecido por la ISO, a continuación, se expone las limitaciones del personal, elementos tangibles (Hardware), elementos intangibles (Software, Información), infraestructura.

- El personal encargado tiene la responsabilidad de velar por el correcto funcionamiento del servidor y de la o las páginas web alojadas en este.
- En cuanto a los elementos tangibles se tiene todo el hardware que se utilizara en el servidor, es decir, los componentes de los cuales este se conforma este.

- El uso de máquinas virtuales, base de datos, aplicaciones y archivos configurados, entran en funcionamiento en cuanto a la ayuda para levantar la página web que residirá en el servidor y usada posteriormente para las pruebas pertinentes.
- Visto desde la infraestructura, el sitio web está constituida por 3 módulos principales y un servidor los cuales son:
    - **Usuarios:** En este apartado de la página se podrán crear usuarios, permitiendo que los mismo puedan ingresar en el sitio mediante un método de seguridad de autentificación por medio de una contraseña cifrada.
    - **Publicaciones:** En esta sección se permitirá subir imágenes con una pequeña descripción dependiendo del usuario que esté logeado, así como también visualizar las publicaciones de los demás.
    - **Likes:** Este módulo está ligado a los dos anteriores, los cuales dependiendo de quien haya realizado la publicación se visualizará para realizar la reacción a esta.
    - **Servidor:** En el módulo referente al servidor, se tiene una carencia de control en cuanto al tráfico de internet usando los protocolos http, tcp e icmp y a su vez control nulo de los puertos usados.

En cuanto al modelo de red del escenario, los riesgos encontrados se sitúan en la capa de transporte y aplicación los cuales son los siguientes:

Capa de Transporte

- Lectura de paquetes enviados por el cliente y servidor.
- Suplantación de servidor o cliente.
- Alteración de paquetes.
- Ataque de denegación de servicios (DOS).
- Ataque por contraseñas (Fuerza Bruta).
- Ataque de hombre en el medio (Man in the Middle).
- Ataque por análisis de tráfico (Sniffer).
- Interceptación no autorizada de datos.
- Espionaje.
- Análisis de tráfico.

Capa de Aplicación

- Solicitudes PDF GET, HTTP GET, HTTP POST, en formularios del sitio web (inicio de sesión, carga de fotos / videos, envío de comentarios).
- Los problemas de diseño abierto permiten el uso gratuito de los recursos de la aplicación por partes no deseadas.
- Los controles de seguridad inadecuados fuerzan el enfoque de «todo o nada», lo que resulta en un acceso excesivo o insuficiente.
- Los controles de seguridad de aplicaciones demasiado complejos tienden a pasarse por alto o no se comprenden e implementan bien.

2.2.11.2.1. Análisis y Evaluación de Riesgos

Existen varios tipos de riesgos, pero en esta investigación se centrará en la categorización y análisis de los riesgos en el servidor, dado a que es la parte fundamental del sitio, ya que este maneja todos los procesos, reglas, información de base de datos, recursos, seguridad, etc.

Tabla 1: Identificación y Categorización de riesgos

Nº	Categoría	Riesgo
1	Servidor	Lectura de paquetes enviados por el cliente y servidor
2	Servidor	Suplantación de servidor o cliente
3	Servidor	Alteración de paquetes
4	Servidor	Ataque de denegación de servicios (DOS)
5	Servidor	Ataque por contraseñas (Fuerza Bruta)
6	Servidor	Ataque de hombre en el medio (Man in the Middle)
7	Servidor	Ataque por análisis de tráfico (Sniffer)
8	Servidor	Interceptación no autorizada de datos
9	Servidor	Espionaje
10	Servidor	Solicitudes PDF GET, HTTP GET, HTTP POST.
11	Servidor	Uso gratuito de los recursos de la aplicación por partes no deseadas.
12	Servidor	Los controles de seguridad inadecuados
13	Servidor	Los controles de seguridad de aplicaciones demasiado complejos

Fuente: Elaboración propia.

En la tabla anterior se detalla los riesgos existentes junto a su debida categorización, en este caso como se mencionó antes, se centrará en la categoría del servidor.

Tabla 2: Estimación de probabilidad sobre los riesgos

Tabla de estimación de probabilidad	
Categoría	**Relación**
Bajo	Se presentan aproximadamente una vez cada año.
Medio	Se presentan aproximadamente una vez cada mes.
Alto	Se presentan aproximadamente una vez cada semana.

Fuente: Elaboración propia.

En la tabla descrita anteriormente se detalla la probabilidad de que un evento ocurra, siendo estos categorizados por; bajo, medio y alto respectivamente.

Tabla 3: Estimación del impacto sobre los riesgos

Tabla de estimación de impacto	
Categoría	**Relación**
Bajo	El daño de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	El daño de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	El daño de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: Elaboración propia.

En la

Tabla *3*: Estimación del impacto sobre los riesgos se detalla el impacto que tendrá un riesgo o evento determinado, previamente descrito.

Tabla 4: Relación Probabilidad e Impacto

		Impacto		
		Bajo	Medio	Alto
Probabilidad	Bajo	Muy Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Muy Alto

Fuente: Elaboración propia

La norma de identificación de los riesgos establece que, en caso de ocurrencia de un riesgo de intensidad BAJA, no es necesaria la corrección inmediata, pero si la toma de alguna medida de protección y en caso de un riesgo con intensidad MEDIA o ALTA, buscar las medidas correctivas para evitar que la consecuencia de alguna de estas nos lleve a la pérdida de información.

2.2.11.3. Fase 3: Identificación de Soluciones

En base a los problemas ya mencionados seguidos de su impacto correspondiente en este escenario, la solución se basa en el uso de aplicaciones y configuraciones las cuales permitirán brindar control y limitaciones en cuanto al tráfico de los protocolos antes mencionados. Más adelante en el apartado de **Solución de la problemática** se detalla la aplicación y puesta en marcha de la solución prevista para mitigar en cierta medida los ataques al servidor.

Según investigaciones realizadas, destacan soluciones basadas en la nube web tales como; Azure web Firewall, Cloudflare, ModSecurity, entre otras, las cuales otorgarían una mejor solución posible a los riesgos identificados en los puntos anteriores, no obstante, es de tener presente que estas alternativas requieren de un abono monetario para su uso. A su vez de la posibilidad de implementar sistemas de captcha los cuales validan que el tráfico generado sea el de un usuario real quien intente ingresar al servidor o página web.

También tener en cuenta que es necesario llevar a cabo una evaluación periódica

sobre el hardware en el servidor para así prevenir posibles daños en cuanto a componentes que impidan el correcto funcionamiento de los mismos.

Tabla 5: Tratamiento de riesgos

Riesgos				
Descripción del riesgo	**Nivel**			**Observaciones**
	B	**M**	**A**	
Lectura de paquetes enviados por el cliente y servidor	x			Cifrar los paquetes enviados.
Suplantación de servidor o cliente			x	Mejorar los protocolos de seguridad.
Alteración de paquetes			x	Aplicar un protocolo de seguridad.
Ataque de denegación de servicios (DOS)			x	Limitar las consultas hechas por un usuario.
Ataque por contraseñas (Fuerza Bruta)		x		Añadir notificaciones de inicios de sesión desde dispositivos desconocidos.
Ataque de hombre en el medio (Man in the Middle)		x		Utilización de un VPN y uso de formatos específicos de datos entrantes.
Ataque por análisis de tráfico (Sniffer)	x			Usar un VPN.
Interceptación no autorizada de datos		x		Cifrar los datos manejados.
Espionaje		x		Cifrar la información del servidor.
Solicitudes PDF GET, HTTP GET, HTTP POST.		x		Validar los datos entrantes de las peticiones con un formato específico.
Uso gratuito de los recursos de la aplicación por partes no deseadas.	x			Liminar el uso de los recursos por usuario.
Los controles de seguridad inadecuados		x		Rectificar los controles de seguridad.
Los controles de seguridad de aplicaciones demasiado complejos		x		Cifrar los paquetes enviados.

Fuente: Elaboración propia.

Según la **Tabla 5:** Tratamiento de riesgos es el anexo para poder realizar el tratamiento de riesgos una vez estos hayan sido identificados y su nivel de probabilidad e impacto.

2.2.11.3.1. Eventos Activadores

Esta clase de eventos pueden ocasionar la activación de una falla crítica o de un riesgo, son determinados en base a la observación y la socialización conjunta con el personal encargado del servidor, como también a través del análisis de los archivos log sirviendo estos como receptores de las actividades realizadas. Dichos eventos se los detalla a continuación:

- Intento de accesos no autorizados a la red para provocar colapso en servicios o robar la información que se mantiene.
- Picos en las visitas realizadas al sitio en determinados horarios o temporadas del año.
- Fallos en el hardware que hospeda el sitio web, ocasionados por condiciones climáticas o eventos de este estilo.
- Actualizaciones realizadas al sitio sin un debido procedimiento y confirmación de fallos.
- Identificación de problemas que no hayan podido ser detectados de forma más temprana.
- Mal funcionamiento en los controles de acceso en las conexiones entrantes de direcciones u ordenadores.
- Falla con la infraestructura de la empresa pública proveedora de servicios básicos hacia la organización (comunicaciones, energía eléctrica, telefonía, entre otros).

2.2.11.4. Fase 4: Estrategias

2.2.11.4.1. Actividades Importantes

- Hay que mantener una revisión de los procesos internos, de la forma en que se llevan, responsables, funciones, dependencias, nivel de importancia.
- Buscar el establecimiento de soluciones de acuerdo a las personas y funciones, además de basarse en áreas donde estén mucho más enfocados los riesgos de ocurrencia de problemas y contingencias para establecer estrategias globales.
- Buscar la aprobación de parte de grandes cargos de la organización, para poder tener la apertura de aplicación de estrategias y en el caso de necesitar un financiamiento, poder establecer dichas soluciones.

- Identificar los beneficios que serán traídos a la organización mediante la aplicación de las estrategias para mejorar aspectos claves de la misma.

2.2.11.5. Fase 5: Documentación del Proceso

La documentación del plan de contingencia es un proceso en donde se identifica todo lo descrito anteriormente desde la **Fase 1: Planificación** hasta la **Fase 4: Estrategias** y se va a ir desarrollando en el transcurso del documento.

2.2.11.6. Fase 6: Realización de Pruebas y Validación

En base a la norma ISO 27001, se recalca que la validación deberá ser ejecutada por parte de un auditor especializado de esta normativa, cuya finalidad es la de conocer si está bien planteado lo descrito en fases anteriores. Para poder tener buenas alternativas, se debe de contar con planes de administración de emergencia o recuperación ante algún fallo suscitado, de lo contrario se puede investigar y definir alternativas de solución.

2.2.11.6.1. Actividades Previas al Desastre

Las actividades a llevarse a cabo buscan la reducción de daños en un desastre, en este caso, preparar y planificar actividades para poder evitar que una denegación de servicio se prolongue. Para una buena práctica, se definen procedimientos formales para cumplir las actividades previas a un desastre, tales como:

Establecimiento de Plan de Acción

Llegados a este punto, los procedimientos y actividades que intervienen son:

Por parte de desastres físicos:

Una revisión periódica de los componentes que maneja el sistema para su funcionamiento, esto con el fin de obtener información que revele los posible desastres que se puedan presentar en las partes físicas, para así poder aplicar su debido mantenimiento y evitar que se produzca un problema más grande en el sistema que entorpezca el correcto funcionamiento de éste.

Por parte de desastre de infraestructura:

Realizar una revisión anual de los módulos que componen el sistema, para encontrar fallas de seguridad en este, además, mantener actualizado los componentes con las nuevas tecnologías ya que estas pueden originar incompatibilidades con las que se podría usar para realizar un ataque externo al sistema.

Por parte de ataques del servidor:

Mantener un monitoreo periódico de las actividades realizadas en el servidor, en cuanto a las entradas y salidas de peticiones, tráfico de internet, uso de puertos para la navegación u otras actividades por parte de los usuarios hacia este al momento de acceder a la página situada en el mismo o uso de algún otro servicio existente.

Por parte a pérdida de información:

- Actualización periódica de los protocolos de acceso a la información.
- Definición de roles para el acceso a la información a nivel de organización y servidor.
- Gestión y descontaminación de dispositivos externos que hayan pasado por una revisión previa de acceso.
- Realización de respaldos periódicos en caso de pérdida en alguna unidad de almacenamiento.
- Revisión de normas y procedimientos (Políticas).
- Informes de cumplimientos o no de las normas y políticas de acción.

2.2.11.6.2. Actividades Durante el Desastre

Plan de Emergencias y o Respaldo

Dependiendo de la catástrofe que se suscite, ya sea esta de manera que afecte a los dispositivos físicos o afecten directamente al servidor en cuestión de software, se debe proceder con la mayor cautela posible para pensar con claridad y así poder mitigar el riesgo.

- **En caso de desastres físicos:** Se deberá evaluar los daños recibidos a los equipos y el personal encargado de la administración de estos, para poder tener en consideración el grado de afectación y posteriormente realizar los respectivos reemplazos en caso de ser necesario.

- **En caso de un ciberdelito:** Según sea el caso, en cuanto a robo, pérdida de información o también una denegación de servicio, ejecutar las estrategias de mitigación descritas en el apartado de **Solución de la problemática** con la intención de detener a tiempo el evento suscitado.

- **En caso de un desastre de infraestructura:** Si llegase a darse el caso de que surjan problemas en cuanto a alguno de los módulos presentes en la página usada por los usuarios, pausar el funcionamiento del servicio de la página y evaluar los módulos para hallar el afecto, luego de realizar dicha comprobación, aplicar las debidas correcciones o soluciones necesarias e iniciar las actividades del sitio web lo antes posible para no perder ninguna información importante.

Formación de Equipos y Entrenamiento

En este punto pueden establecerse los equipos equipo no numeroso de personas internas que monitoreen el comportamiento de los objetos estudiados por parte del plan y les den su propio seguimiento. Para la optimización de las actividades, es mejor tener dos grupos trabajando tanto en la mitigación del evento suscitado como también de proteger los datos, servicios y recursos que sean posibles durante la ocurrencia de dicho evento. Sobra decir que, para la formación de los grupos mencionados, estos deben de estar en contraste aprendizaje de su entorno, es decir, investigar nuevas formas de resolver algún problema presentado y evitar los máximo posible el número de pérdidas.

2.2.11.6.3. Actividades Después Desastre

Una vez que el problema o catástrofe se ha presentado en el escenario y a su vez habiendo seguido las debidas correcciones que se han planteado anteriormente, hay que realizar las evaluaciones de resultados que ha dejado el suceso tales como:

- **Evaluación de Daños**

Es pertinente realizar una valoración y evaluación de los daños reportados ante los eventos suscitados en la contingencia, para determinar el impacto que estos han tenido en el escenario planteado y priorizar la recuperación del servicio en la menor cantidad de tiempo posible.

- **Ejecución de Actividades**

En este caso de haber encontrados los daños pertinentes y habiéndolos clasificados y evaluados por parte de la persona grupo de personas encargadas de la administración de la página y servidor deben realizar las actividades pertinentes para la recuperación de la organización después de haber pasado el evento determinado, ya que es necesario el funcionamiento normal y continuo de la misma con la finalidad de evitar que su funcionamiento de sus actividades se vea afectado y a su vez evitar pérdidas de cualquier tipo.

- **Evaluación de Resultados**

Después de los acontecimiento presenciados en el escenario, la denegación de servicios quedo controlada en cierta medida, si se observa el apartado de **Resultados de la solución** se puede evidenciar que en cuanto al funcionamiento de la página y servidor no se vieron afectados ya que se ejecutaron los controles descritos con éxito.

- **Retroalimentación**

Tomar en cuenta todos los pasos anteriores, para así elaborar informes pertinentes que sirvan de rica de los sucesos pasados, cuáles fueron las medidas adoptadas, cuál fue el daño generado, y si la recuperación dependía de mucho o mediano esfuerzo para poder realizarla.

2.2.11.7. Fase 7: Implementación

Esta fase es el plan de acción una vez que se ha desatado una contingencia y es para lo que las 6 fases anteriores de la metodología han estado preparando al escenario. Aquí es el momento de cuando ocurra o esté por ocurrir la contingencia deben tenerse presente los planes mencionados que se ejecutarán, las medidas adecuadas que van a ser útiles para cada proceso y de qué forma y orden deben ejecutarse.

2.2.11.8. Fase 8: Mantenimiento

Llegando al final del plan de contingencia, la última fase se enfoca llevar un monitoreo sobre los acontecimientos suscitados durante la puesta en marcha del plan y a su vez en determinado tiempo realizar cambios en la documentación con nuevos estudios y nuevas formas o planes de acción para poder mitigar nuevas anomalías encontradas que puedan afectar el rendimiento del servidor y a su vez de la página alojada en este. Cabe aclarar que tanto la fase 7 como la fase 8 no van a ser ejecutadas en la presente investigación, por tanto, únicamente se nombra el rol que tienen dentro de la metodología.

2.2.12. Políticas de seguridad

Cuando se piensa en seguridad y plan de contingencia, se debe de definir procedimientos, normativas y controles que permitan tomar acciones y de cierto modo tener registro de las actividades que se suscitan en cierto momento [30] Todo esto para poder identificar brechas, amenazas y vulnerabilidades que puedan llegar a afectar significativamente de forma negativa a una empresa y a todos quienes la conforman. Dentro de las políticas de seguridad, se debe definir mecanismos que ayuden a detectar ciertas actividades maliciosas, estos se los hacen con el fin de anticiparse a los eventos y evitar que se efectúen y puedan dañar la integridad ya sea física o lógica de los sistemas. [29]

De igual manera, al definir políticas de seguridad para una aplicación o una empresa, es importante tener en cuenta metodologías, normativas y técnicas [31] las cuales facilitan el enfoque que se les dará a las mismas, esto se toma en cuenta al momento de recibir evaluaciones por otras entidades dedicadas a estas actividades. Esta definición de políticas conlleva un proceso detrás de estas, ya que se debe primero identificar las falencias existentes que puedan provocar daños graves.

2.3. OBJETIVOS DEL PROTOTIPO

2.3.1. Objetivo General

Crear un plan de contingencia, mediante la simulación de ciberataques a sitios web, para la detección de anomalías y mejora de seguridad.

2.3.2. Objetivos Específicos

- Recopilar información en bases bibliográficas, libros, artículos científicos, entre otros, para la fundamentación teórica de la investigación.
- Determinar los tipos de ataques DDos, mediante el uso de las herramientas, que permitan denegar el servicio al sitio web.
- Utilizar los ataques http flood, ping de la muerte al sitio web de prueba, para identificar y analizar cada una de las respuestas de seguridad informática frente a los riesgos en la aplicación web.
- Elaborar, con los resultados obtenidos, un plan de contingencia que ayude a mitigar todo tipo de fallos que den acceso viable a un ataque externo en la aplicación con acceso a internet.

2.4. DISEÑO DEL PROTOTIPO

2.4.1. Software de Virtualización

Para el proceso de pruebas se opta por usar VMware Workstation con varias ventajas destacables frente a sus competencias. Es desarrollada por VMware, Inc. Es un software de pago, pero también existe su versión no comercial llamada VMware Player, permite a los usuarios crear y configurar máquinas virtuales (VM) en una sola máquina física y usarlas simultáneamente junto con la máquina host.

2.4.2. Sistema Operativo

2.4.2.1. Kali Linux

Kali Linux es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa.

2.4.2.2. Windows

Sistema operativo más utilizado desarrollado por la empresa Microsoft Corporativos, este sirve como puente entre una persona y un ordenador, pudiendo así configurarlo en base a las necesidades que el usuario necesite.

2.4.3. Aplicaciones

2.4.3.1. Low Orbit Ion Cannon (LOIC)

Es una de las aplicaciones usadas para la denegación de servicios distribuida, cuyo objetivo es el de interrumpir el servicio con él envió de paquetes tcp, udp o http. [32] Se hizo famosa por el ataque “Operation Payback” [33], es fácil de usar, pero también fácil de ser detectada al no ocultar la dirección del ataque.

2.4.3.2. HTTP Unbearable Load King (HULK)

Al igual que el anterior, este es un programa usado para realizar ataques DDos a un servidor, creando muchas solicitudes http. [34] En comparación con otras aplicaciones del mismo propósito, Hulk se destaca con ser más sutil al momento de dejar rastros, es decir, deja un patrón único en cada petición que manda al servidor, esto se lo hace para no crear patrones repetitivos y dificultar la detección.

2.4.3.3. Tor’s Hammer

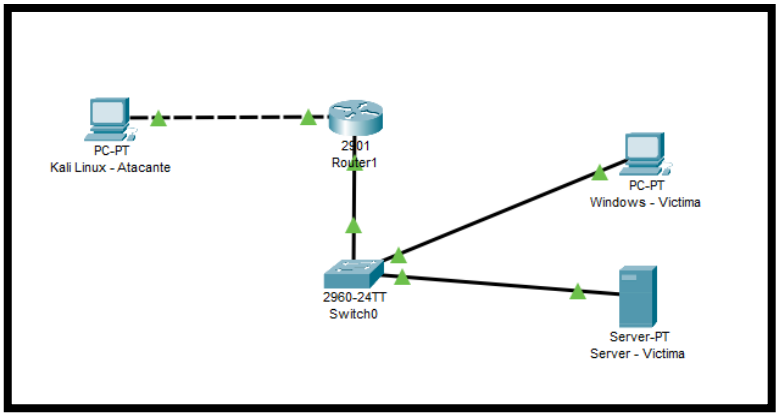
Tor’s Hammer puede ser usado mediante la red para su difícil detección. Lo que simula hacer es un ataque de múltiples peticiones http, estas son enviadas de manera incompleta y a su vez de forma lenta para poder tener una conexión de larga duración. Todo eso con el objetivo de que el servidor no pueda tener más conexiones activas, por entre se saturará y se caerá. [35]

2.5. EJECUCIÓN Y/O ENSAMBLAJE DEL PROTOTIPO

2.5.1. Construcción del escenario

En el desarrollo práctico de esta investigación, se optó por aplicaciones que ayudarán a la ejecución y puesta en marcha de la solución que se plantea, el escenario que se tiene previsto es el siguiente:

Ilustración 2: Escenario de pruebas.



Fuente: Elaboración propia.

2.5.1.1. Direccionamiento IP

Tabla 6: Direccionamiento IP de las máquinas usadas.

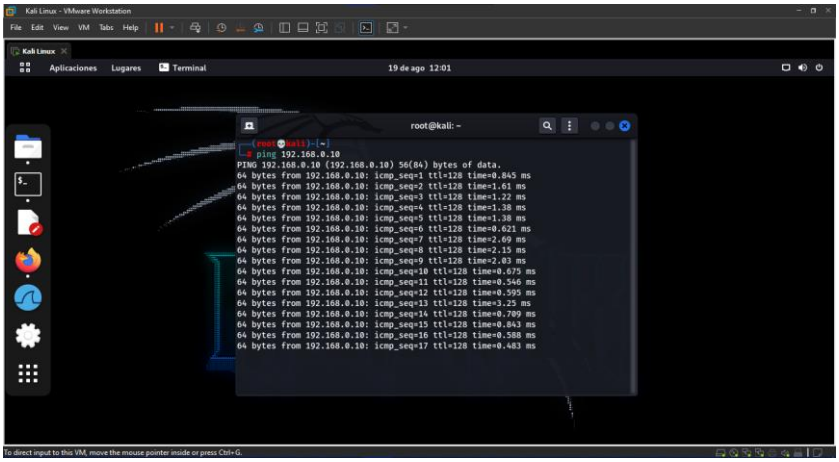
Sistema Operativo	Dirección IP	Máscara de Subred	Puerta de enlace
Servidor	192.168.0.10	255.255.255.0	192.168.0.1
Kali Linux	192.168.0.100		

Fuente: Elaboración propia.

2.5.1.2. Pruebas de conexión entre ambas máquinas

Testeo de conexión entre la máquina atacante hacia la atacada con la herramienta ping.

Ilustración 3: Verificación de conexión desde la máquina atacante.



Fuente: Elaboración propia.

En este caso se realizó una prueba con la herramienta desde la máquina atacante hacia la atacada con el fin de poder verificar la conexión entre máquinas.

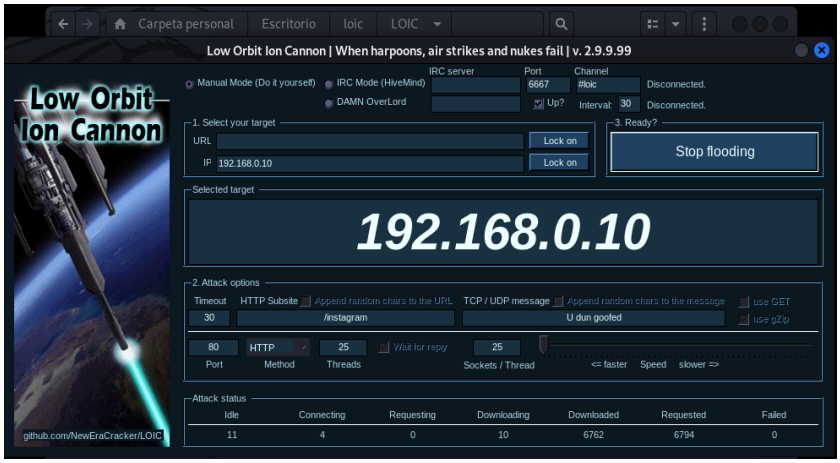
2.5.2. Desarrollo y resultados de ataques Dos al servidor

Se realizarán varios ataques al servidor web para obtener datos sobre los fallos y posibles vulnerabilidades existentes.

2.5.2.1. Ataque con LOIC

En este caso lo que se va a hacer es atacar a una página web con una determinada dirección IP montada en el servidor de pruebas. Para su uso se configura los parámetros dependiendo la cantidad de hilos y cantidad de computadores virtuales para poder mandar peticiones de tipo http e intentar hacer caer la página consumiendo recursos del servidor.

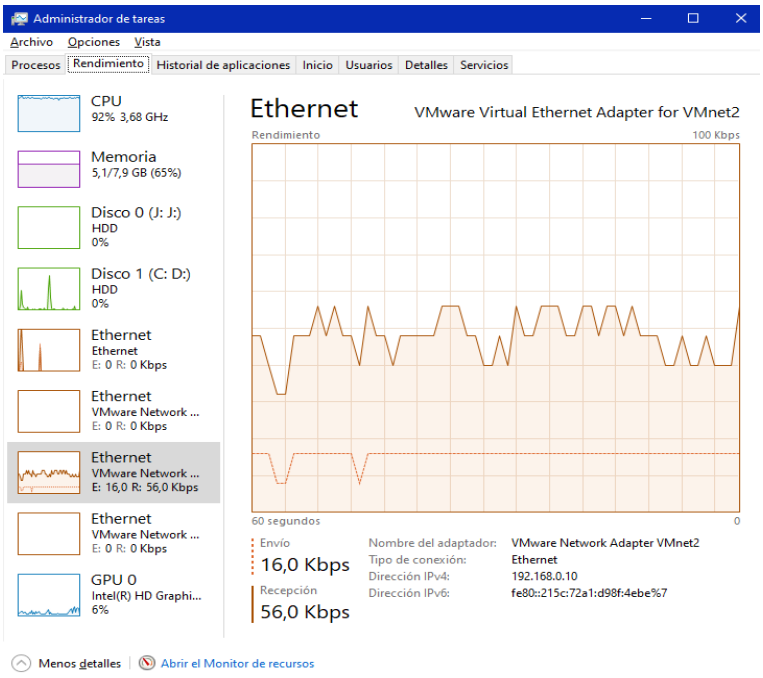
Ilustración 4: Herramienta LOIC en ejecución.



Fuente: Elaboración propia.

Una vez configurado todos los parámetros necesarios, se da inicio al ataque con la aplicación, entre las configuraciones se puede elegir entre diferentes protocolos a usar en las pruebas.

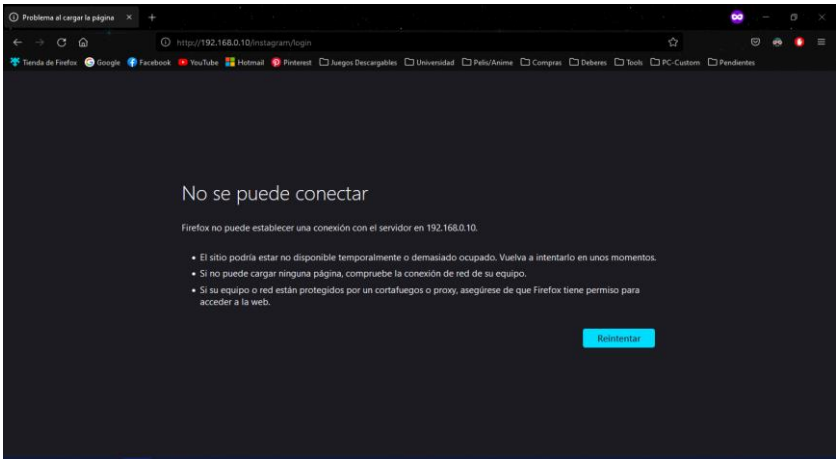
Ilustración 5: Consumo de recursos de la máquina víctima.



Fuente: Elaboración propia.

Una vez puesto en marcha el ataque al ancho de banda de la víctima, podemos revisar en el administrador de recursos como sube rápidamente el consumo de internet.

Ilustración 6: Denegación de servicio activa en el website de pruebas



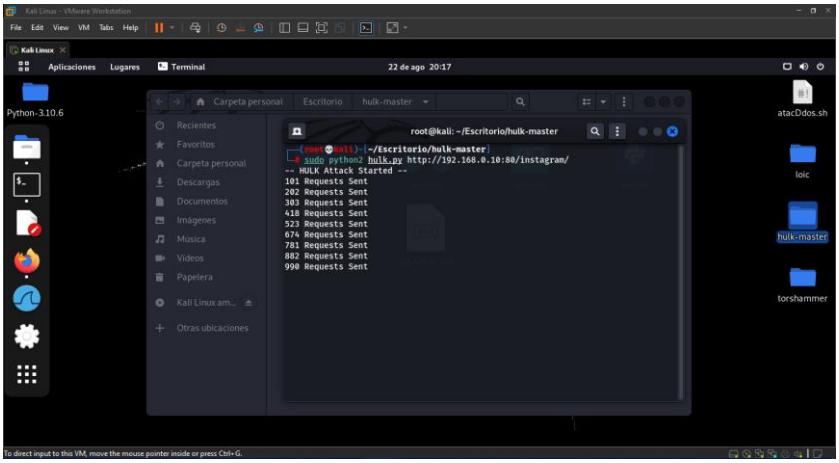
Fuente: Elaboración propia.

Como consecuencia, el usuario no puede acceder al website debido a la saturación del ancho de banda que tiene la víctima como se puede ver en la **Ilustración 5:** Consumo de recursos de la máquina víctima.

2.5.2.2. Ataque con Hulk

Como ya se ha hablado de las funciones de esta herramienta, lo que se hará es crear un mayor número de peticiones al servidor para poder aumentar la carga y con ello hacer que se caiga.

Ilustración 7: Herramienta Hulk en ejecución.



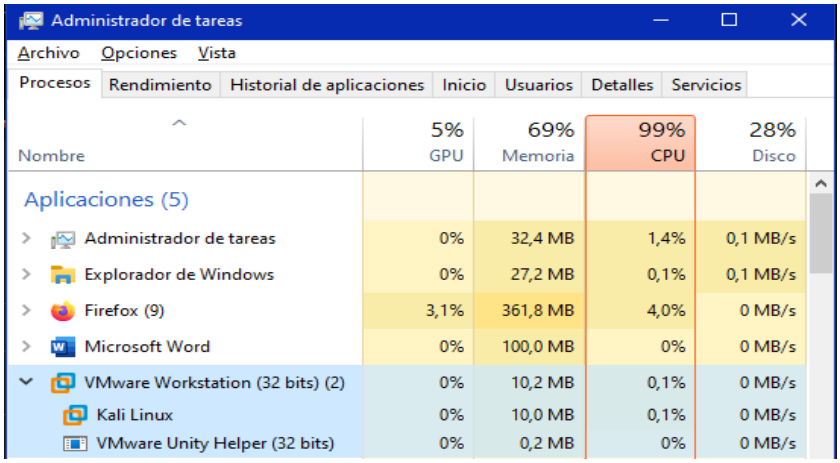
Fuente: Elaboración propia.

Para poder llamar y ejecutar la aplicación hecha en python se realiza lo siguiente:

sudo python hulk.py http://<IP>:<PortNo>/

en donde, solo se necesita la dirección IP o el nombre del dominio del web site acompañada con el número de puertos.

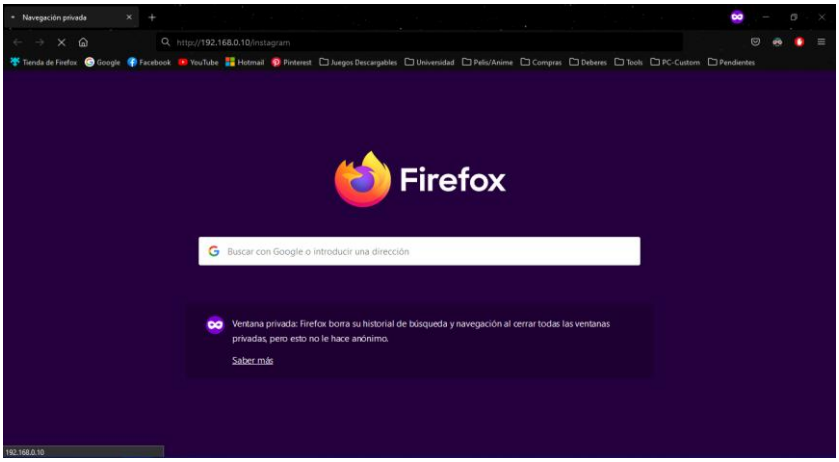
Ilustración 8: Alto consumo de la CPU con el ataque activo.



Fuente: Elaboración propia.

Como se puede apreciar en la imagen anterior, el uso de recursos comienza a elevarse debido a que el ataque está siendo ejecutado.

Ilustración 9: Tiempo de carga extenso con negación de servicio activa.



Fuente: Elaboración propia.

Como consecuencia del ataque ejecutado, la carga del sitio web solo se queda en espera, es decir, tarda demasiado en dar paso a la página principal, lo que nos da a entender que la conexión hacia el servidor está teniendo problemas y posiblemente se caiga.

2.5.2.3. Ataque con Tor's Hammer

Es otra aplicación ejecutada por Python, en donde:

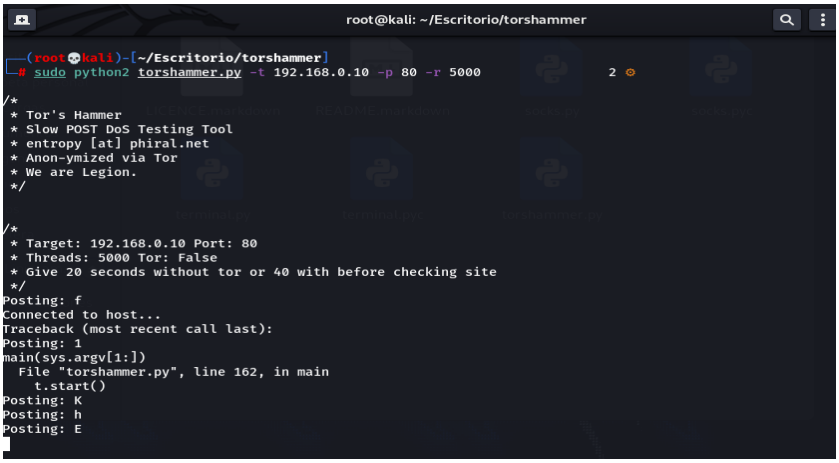
sudo python torshammer.py -t hostname/IP -p 80 -r 5000

-t es el dominio o la dirección IP atacada.

-p es el puerto que por lo general es el puerto 80.

-r es el número de hilos o subprocesos que se desea ejecutar durante el ataque.

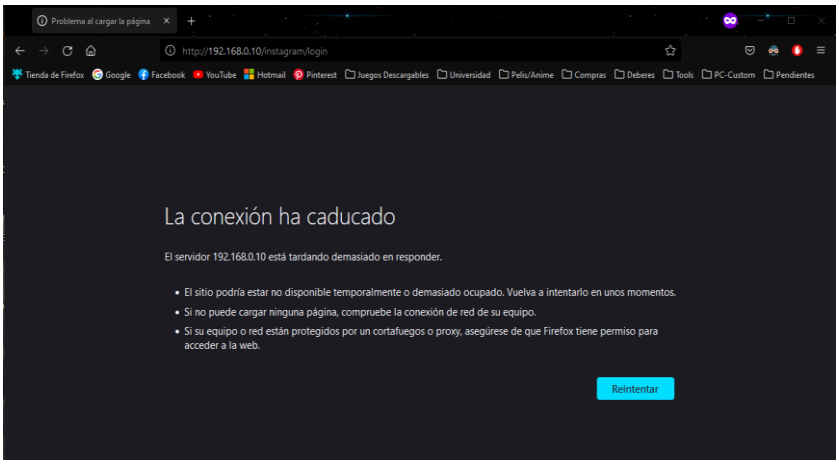
Ilustración 10: Herramienta Tor's Hammer en ejecución.



Fuente: Elaboración propia.

Con la ejecución y especificación de la dirección IP, número de puerto y el número de subprocesos que se desee, se puede llegar a afectar todo el servidor en cuanto al tiempo de respuesta al acceder a alguna página web alojada en este.

Ilustración 11: Negación de servicio activa, tiempo de espera agotado.



Fuente: Elaboración propia.

El resultado era de esperarse, al igual que en la **Ilustración *9*:** Tiempo de carga extenso con negación de servicio activa., el tiempo de conexión de la página web hacia el servidor se ve afectado, arrojando un resultado de una conexión fallida dado a que el tiempo de espera para la conexión se agotó.

2.5.2.4. Ataque con Ping de la muerte

En esta prueba, se intenta saturar el ancho de banda de la víctima en donde:

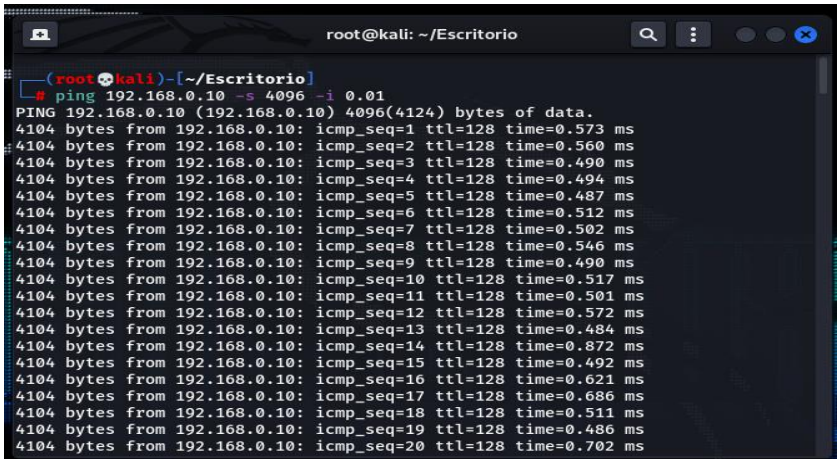
ping hostname/IP -s -i

-s: Indica el tamaño del paquete en Bytes.

-i: Es el tiempo que debe esperar un paquete para poder ser enviado, en este caso no interesa la respuesta, tan solo saturar el servidor.

-f: Ejecuta una inundación ping (flood ping).

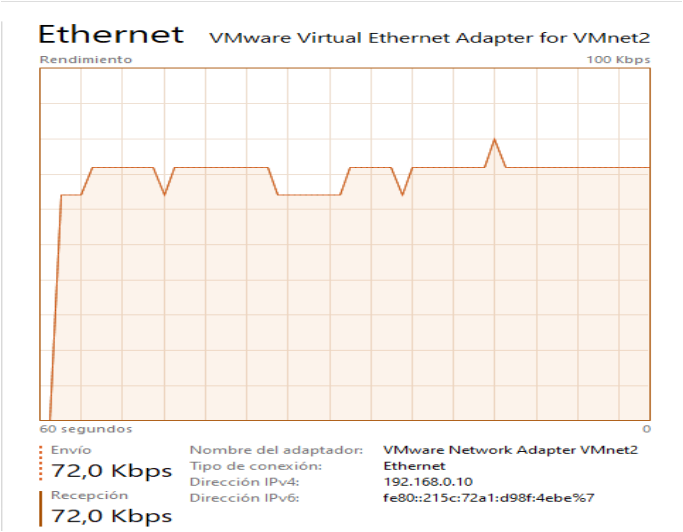
Ilustración 12: Ataque en ejecución.



Fuente: Elaboración propia.

Este es un ataque básico, aunque un poco viejo para poder denegar un servicio, con esto simulamos un eco con el protocolo ICMP para envió de paquetes a la víctima logrando así que se congele o deje de funcionar.

Ilustración 13: Consumo del ancho de banda en la máquina víctima.



Fuente: Elaboración propia.

Justamente como muestra la imagen anterior, la víctima sufre de un elevado ancho de banda debido al ataque ejecutado.

2.5.3. Solución de la problemática

La solución plantea el uso de un firewall el cual consta de una configuración de políticas **iptables** en conjunto con la herramienta **fail2ban**, todo esto situado en un sistema Open Source, con la finalidad de poder controlar el tráfico de la red y así poder cumplir el objetivo planteado.

2.5.3.1. Reglas iptables

Teniendo en cuenta que el tráfico a controlar es en base a los protocolos HTTP, ICMP y TCP, se debe de pensar el uso de políticas que se acoplen a estos para evitar los ataques mencionados con anterioridad y a su vez no dañar la experiencia de navegación. Los parámetros a considerar son los siguientes:

Tabla 7: Descripción de parámetros más usados en reglas de iptable.

Parámetro	Descripción
-p, --protocol	Especifica el protocolo que será parte de la política configurada
-s, --souce	Define el parámetro en cuanto a la IP de entrada
-d, --destination	Define el parámetro en cuanto a la IP de salida
-j	Indica el tipo de acción que se tomara
ACCEPT	Indica que el paquete ha sido aceptado.
DROP	Indica que el paquete ha sido rechazado.
RETURN	El cortafuego deja de ejecutar la siguiente conjunto de reglas y devuelve el control a la chain llamada.
-A, --append	Agrega la regla creada al cortafuegos para determinar la acción sobre los paquetes, esto dependerá si es de **INPUT**, **OUTPUT** o **FORWARD**.
-D, --delete	Elimina la regla creada de cortafuegos, al igual que en el caso de **-A** dependerá también si es de **INPUT**, **OUTPUT** o **FORWARD**.
-I, --insert	Agrega la regla creada en una posición determinada.
-L, --list	Ofrece un listado de todas las reglas creadas dependiendo de la cadena deseada.
-F, --flush	Permite eliminar todas la reglas creadas de una determinada cadena.
-limit 0/s	Indica la tasa de coincidencias media máximas en segundos.
–limit-burst	Indica el número inicial máximo de paquetes que deben coincidir.
-m state — state NEW, ESTABLISHED	Acepta nuevas conexiones y las establecidas.

Fuente: Elaboración propia.

2.5.3.2. Definición de políticas y reglas iptable

Usando parte de los parámetros descritos en la ***Tabla 7*** se construirán reglas que permitan controlar el tráfico de los protocolos empleados en ataques de denegación de servicios para su posterior uso en conjunto a la herramienta fail2ban.

Ilustración 14: Reglas generales para Iptables.

```
  GNU nano 4.8
#!/bin/bash

#Este script establece realiza las siguientes acciones:
#1 borra todas las reglas de iptables de la tabla filter y nat:
#2 establece politicas por defecto a denegar todo el trafico

#eliminar reglas de filer y nat
iptables -t filter -F
iptables -t nat -F

#reincia los contadores
iptables -t filter -Z
iptables -t nat -Z

#politicas por defecto
#denegar todo el trafico en las tres cadenas de filer
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

#Reinicia las politicas por defecto en la tabla Nat.
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

#Borra todas las cadenas que no vienen por defecto con las
#tablas Filter y Nat.
iptables -X
iptables -t nat -X
iptables -t filter -X
```

Fuente: Elaboración propia.

Se definen reglas y políticas generales en iptables, esto está sujeto a cambios, es decir, se puede aceptar o denegar el tráfico tanto entrante como saliente de internet dependiendo de la intención que se haya definido. Esto se lo hace con el fin de buenas prácticas en cuestión de control.

Ilustración 15: Política para syn flood.

```
#limitar numero de conexiones TCP entrantes
iptables -N syn_flood
iptables -A INPUT -p tcp --syn -j syn_flood
iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
iptables -A syn_flood -j DROP
```

Fuente: Elaboración propia.

La definición de esta política cumple con el objetivo de limitar a cierto número de intentos por segundo en cuanto al tráfico del protocolo TCP, este caso la intención se define limitar a 3 intentos por segundo logrando así frenar un ataque de syn flood si llega a surgir este inconveniente.

Ilustración 16: Regla para control de solicitudes ICMP.

```
#limitar numero de solicitudes PING entrantes
iptables -A INPUT -p icmp -m limit --limit  1/s --limit-burst 1 -j ACCEPT

iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j LOG --log-prefix PING-DROP:
iptables -A INPUT -p icmp -j DROP

iptables -A OUTPUT -p icmp -j ACCEPT
```

Fuente: Elaboración propia.

En este caso, se crea una regla que permita el control de solicitudes entrantes del protocolo ICMP usando la herramienta, evitando así que un ataque de ping de la muerte lleve a cabo el objetivo de elevar el consumo de ancho de banda.

Ilustración 17: Regla para control de conexiones entrantes al servidor.

```
#limitar conexion entrante al servidor ssh
iptables -I INPUT -p tcp -s 192.168.0.10 -d 192.168.0.100 --sport 80 --dport 80 -m state --state NEW,ESTABLISHED -m recent --set -j ACCEPT
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 120 --hitcount 5 -j DROP
iptables -A OUTPUT -p tcp -s 192.168.0.10 -d 192.168.0.100 --sport 80 --dport 80 -m state --state ESTABLISHED -j ACCEPT
```

Fuente: Elaboración propia.

En conjunto con las demás reglas la supervisión en cuanto al tráfico del protocolo TCP dependerá de la IP de origen y destino que se haya definido para poder aplicar el control respectivo cuando se lo una a la configuración de otra aplicación.

2.5.3.3. Configuración de Fail2ban

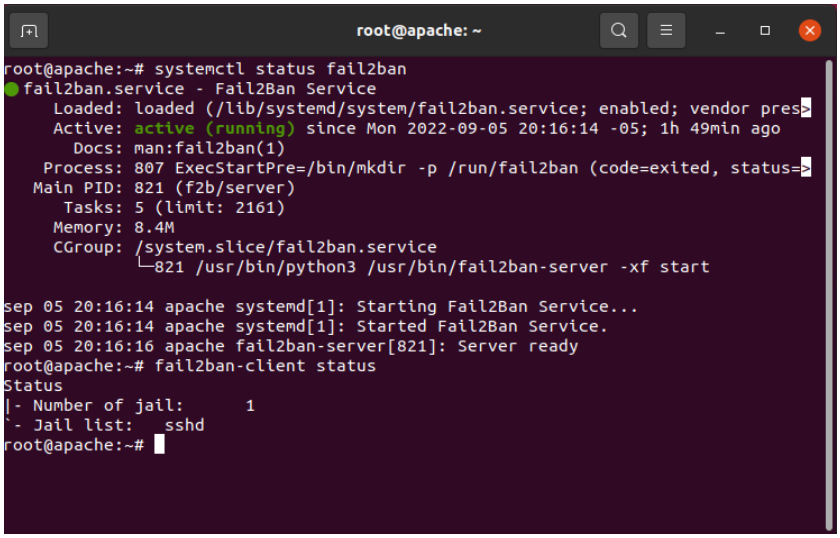
En conjunto con la creación reglas en iptables y configuración de esta aplicación se busca banear la ip por la cual proviene el ataque de denegación de servicio, este baneo dependerá al tiempo que se le haya ajustado en la configuración. En estas configuraciones suelen usarse parámetros para distintas finalidades tales como:

Tabla 8: Parámetros usualmente utilizados en la configuración de fail2ban.

Parámetros	Descripción
ignoreip	Hace referencia a la IP que debe ser ignorada por el sistema de prohibición.
findtime	Contará el número de intentos fallidos en la duración establecida
bantime	Establece la duración de la prohibición en segundos.
maxretry	Indica el número de intentos fallidos soportados.
backend	Es una entrada en donde se especifica como la herramienta supervisará los archivos de registro.
banaction	Estable la acción a tomar cuando se alcance el número de intentos fallidos.
protocolo	Es el tipo de tráfico que se eliminará cuando este activa la prohibición de IP.
cadena	Se configura con una regla de salto para evitar tráfico al embudo fail2ban.

Fuente: Elaboración propia.

Ilustración 18: Estado del servicio de fail2ban



Fuente: Elaboración propia.

Se verifica el estado del servicio para confirmar que este activo y a su vez revisar que configuraciones se activaron por defecto.

Ilustración 19: Configuración del archivo de jaula.

Fuente: Elaboración propia.

Por recomendación y buenas prácticas se crea un nuevo archivo que contendrá la configuración de la jaula que servirá para poder aplicar las acciones de iptables y excluir la dirección IP del atacante.

2.5.4. Resultados de la solución

2.5.4.1. Verificación de reglas aplicadas

Se verifica que la políticas creadas se hayan aplicado con éxito, para esto se usará el siguiente comando:

iptables -L -nv --line-numbers

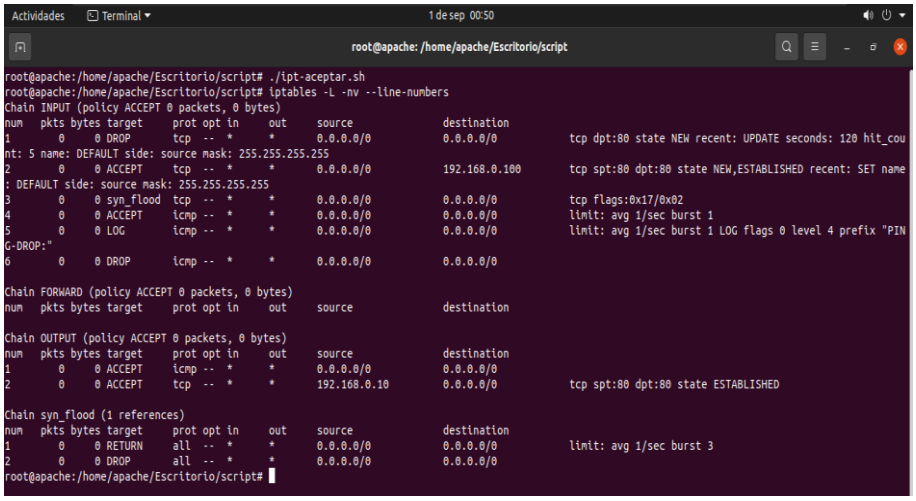
El comando ayuda a visualizar a detalle las reglas existentes en iptables.

Ilustración 20: Iptables sin reglas establecidas.

Fuente: Elaboración propia.

Normalmente las reglas de iptables suelen estar vacías a menos que se hayan configurado otras previamente, en este caso para fines prácticos se ha borrado cualquier otra configuración y solo se ha permitido acceso de entrada como de salida a internet.

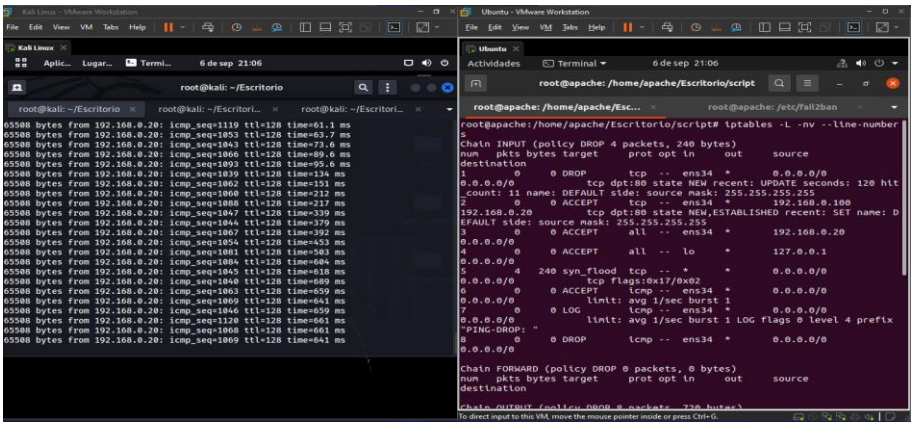
Ilustración 21: Reglas de iptable aplicadas.



Fuente: Elaboración propia.

Lo que se hace es ejecutar un archivo sh el cual tiene todas las reglas previamente configuradas con el fin de poder limitar y a su vez trabajar en conjunto con otras herramientas para controlar el tráfico de los protocolos.

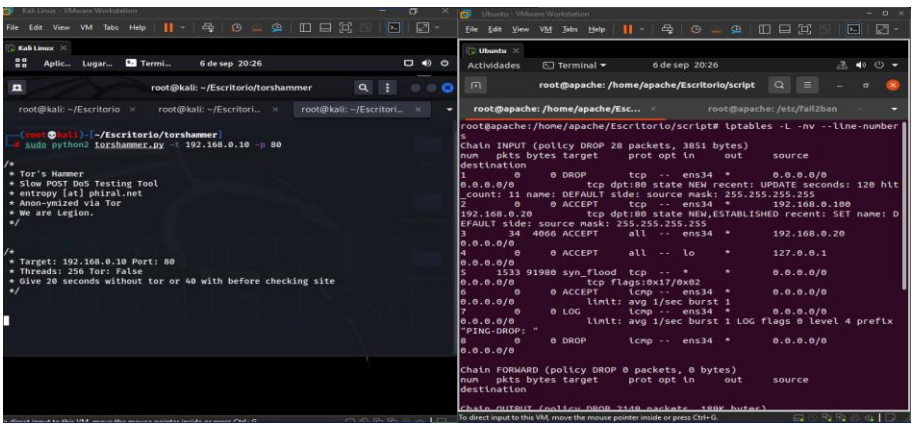
Ilustración 22: Uso del script para ejecutar el ataque de ping de la muerte.



Fuente: Elaboración propia.

Al ejecutar el ataque con el script, se comienza a crear y enviar el número de paquetes descrito rápidamente, pero al detectar el servidor el número paquetes entrantes del protocolo icmp se activa el control de iptables para posteriormente excluir el origen del ataque.

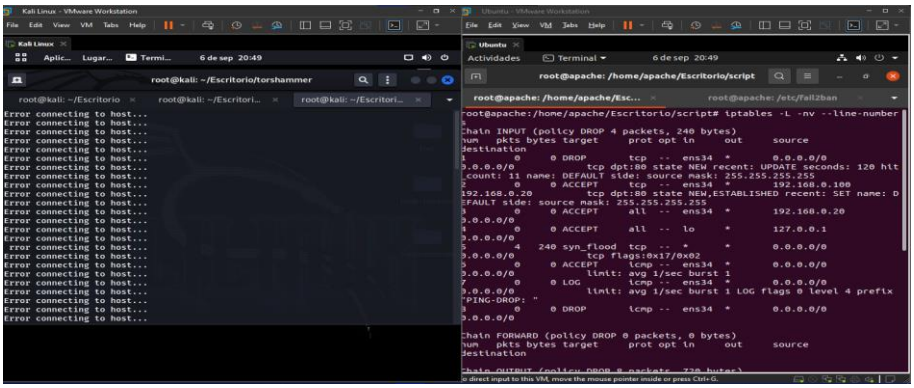
Ilustración 23: Ataque DDos con torshammer.



Fuente: Elaboración propia.

Poniendo en marcha el ataque, se tarda unos minutos para conectarse con el servidor víctima, aquel tiempo se vería reducido al no tener una configuración de seguridad que permita limitar el tráfico y tomar otras medidas en caso de que siga dándose el caso de incumplir las reglas establecidas.

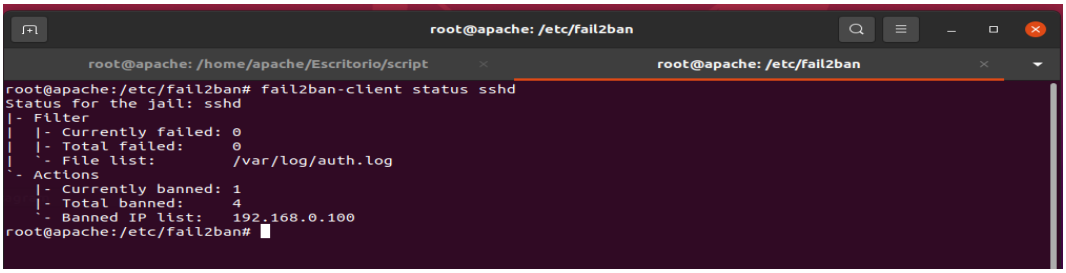
Ilustración 24: Impedimento de la máquina atacante al servidor.



Fuente: Elaboración propia.

El resultado es positivo, como se puede ver las configuraciones impidieron que la maquina atacante se pase del límite de peticiones establecidas.

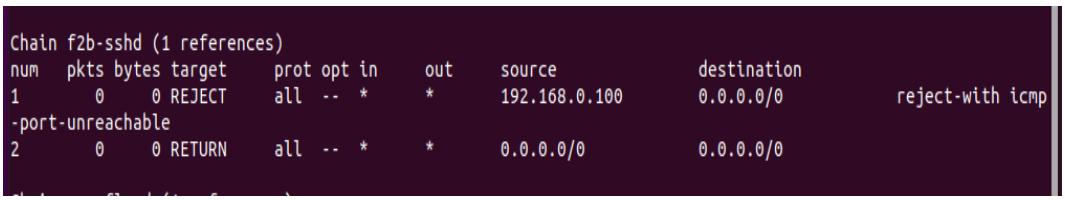
Ilustración 25: Estado actual tras el ataque de la ip de origen.



Fuente: Elaboración propia.

Se actualiza el estado del servicio para poder revisar si la configuración en conjunto de iptables y fail2ban ha surgido efecto.

Ilustración 26: Resultado de la ip excluida mostrada en iptables.



Fuente: Elaboración propia.

Como se puede ver, al excluir la ip de origen de la maquina por la que se está efectuando el ataque de denegación de servicio, automáticamente se crea una política por la cual se visualiza la exclusión de dicha Ip para entrar al servidor.

3. CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

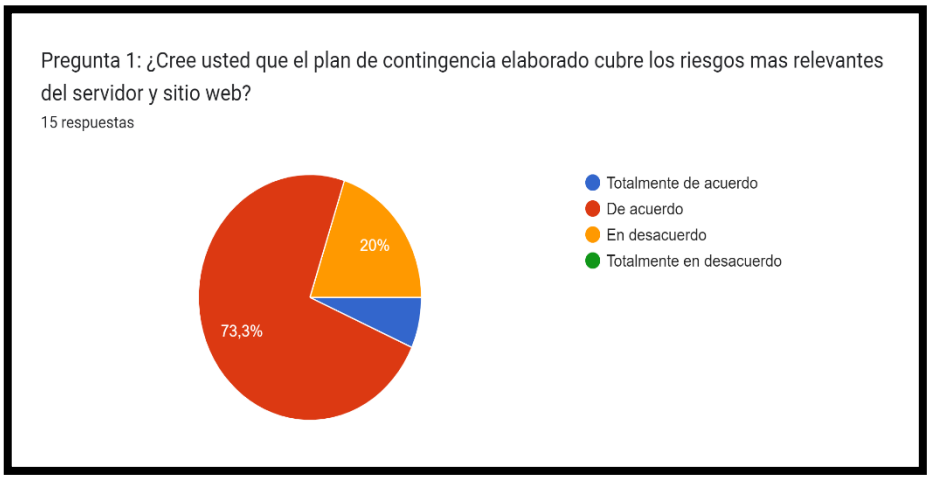
3.1. PLAN DE EVALUACIÓN

Se propone crear un plan de contingencia el cual ayude a controlar y reducir ataques de denegación de servicios, esto se ha basado principalmente en el uso de herramientas que ayuden a explotar fallos existentes de un sitio web, para que con todo esto, se pueda tomar las medidas respectivas ante futuros ataques similares.

3.2. RESULTADOS DE LA EVALUACIÓN

Durante la creación del plan de contingencia, este mismo se sometió a una revisión y evaluación en conjunto con especialistas en esta área, los cuales respondieron a una encuesta, encontrada en el **Anexo 1: Encuesta a especialistas** para lo cual los resultados evaluados en cuanto a la fiabilidad de la solución planteada fueron los siguientes:

Ilustración 27: Pregunta 1 del anexo de evaluación del especialista



Fuente: Elaboración propia.

Como resultados de la primera pregunta se puede visualizar que mas del 50% de los participantes respondieron positivamente en cuanto al rango relevante de riesgos en el plan desarrollado.

Ilustración 28: Pregunta 2 del anexo de evaluación del especialista

Fuente: Elaboración propia.

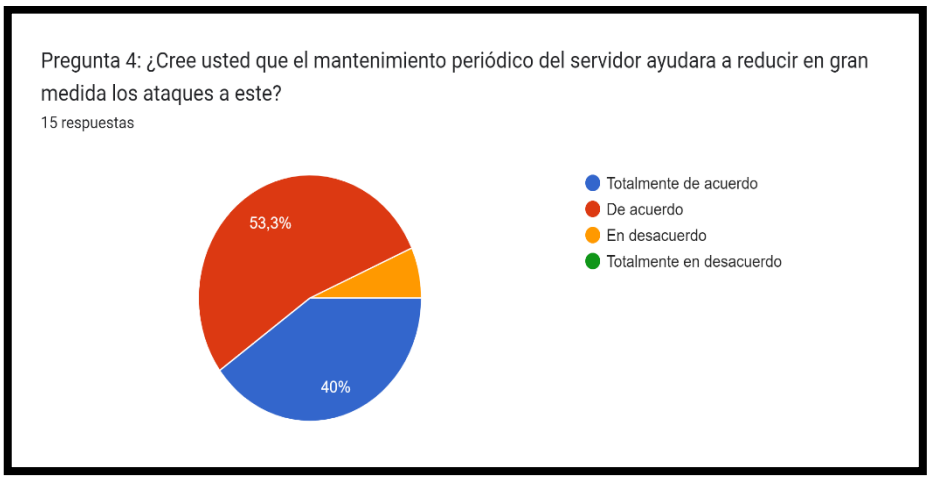
Dada la opinión de los participantes, se mostraron de acuerdo a la idea respecto a la exclusión de direcciones IP's provenientes de atacantes como una manera de mitigar los ataques DoS.

Ilustración 29: Pregunta 3 del anexo de evaluación del especialista

Fuente: Elaboración propia.

Los resultados de la pregunta 3 demuestran que un 60% de los participantes, están de acuerdo considerando que la relación de probabilidad e impacto asignada a los riesgos encontrados es correcta, pero también una menor parte están en desacuerdo ya que existen riesgos que se consideran como más dañinos que otros a no ser resueltos y suscitarse un evento con dichos riesgos.

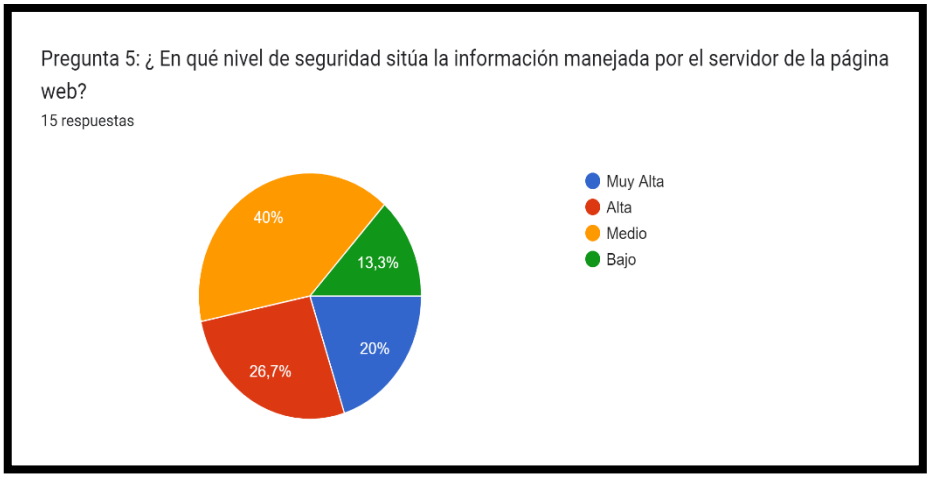
Ilustración 30: Pregunta 4 del anexo de evaluación del especialista



Fuente: Elaboración propia.

Mas del 50% de las personas involucradas en la encuesta, les parece una buena medida de reducir ataques y eventos asociados con intenciones maliciosas.

Ilustración 31: Pregunta 5 del anexo de evaluación del especialista



Fuente: Elaboración propia.

Un 40% de los especialistas concuerdan que el servidor se encuentra situado en un nivel medio de seguridad, pero a su vez, recalcan que no siempre se situara en ese nivel, dado al constante cambio respecto a la tecnología, los controles implementados en la seguridad se volverán obsoletos debido a dichos avances.

CONCLUSIONES

- Se recopiló información en distintas fuentes bibliográficas, esto permitió fundamentar teóricamente toda la investigación realizada ya que sirvió como base para el desarrollo de la misma, tomando en cuenta acontecimientos e información importante de hechos pasados.

- Determinando los tipos de ataques Dos se pudo utilizar herramientas varias, permitiendo así llegar a los resultados esperados, es decir, ejecutar una denegación el acceso a una página web.

- Al momento de utilizar los ataques http flood, ping de la muerte se pudieron encontrar vulnerabilidades frente a distintos tipos de riesgos en la seguridad informática, los resultados obtenidos pueden ayudar a obtener las soluciones.

- Se elaboró un plan de contingencia que ayudó a mitigar los fallos y cubrir los rangos de acceso para un ataque por parte de uno o varios usuarios externos.

RECOMENDACIONES

- Llenarse de información fiable acerca de lo que esté sucediendo durante un ciberataque de cualquier tipo, ayuda a poder pensar con claridad al momento de tomar decisiones de cómo poder resolver el problema, tanto como para una empresa como para un usuario normal.
- Usar las herramientas y recursos tecnológicos que sean necesarios para poder aumentar el nivel de seguridad en los sitios web y servidores para prevenir ser víctimas de hackeo. En caso de ser víctimas de hackeo, tomar las medidas respectivas para solucionar el problema en la mayor brevedad posible, ya que pueden traer repercusiones futuras.
- Tener precaución sobre la información proporcionada en páginas que se visitan diariamente en internet, ya que estas pueden tener una mala reputación y en consecuencia de esto pueden ser víctimas de delitos informáticos.
- No toda solución es definitiva ni el uso de una herramienta o servicio garantiza resolver con certeza algún problema sobre ciberdelitos, infraestructura o algún otro, por ello es necesario tener varios puntos de vista a considerar para implementar una solución que ayude en su gran mayoría a problemas existentes y futuros.

BIBLIOGRAFÍA

[1] A. Jaszcz y D. Polap, «AIMM: Artificial Intelligence Merged Methods for flood DDoS attacks detection,» *Journal of King Saud University - Computer and Information Sciences,* p. 12, 27 Julio 2022.

[2] D. Nashat y F. A. Hussain, «Multifractal detrended fluctuation analysis based detection for SYN flooding attack,» *ELSEVIER,* vol. 107, p. 102315, 01 Agosto 2021.

[3] M. Linares Vásquez, «ESET Latinoamérica presenta el estudio ESET Security Report 2021,» 16 Mayo 2021. [En línea]. Available: https://www.segurilatam.com/actualidad/eset-latinoamerica-presenta-el-estudio-eset-security-report-2021_20210516.html#:~:text=Ciberseguridad%20ESET%20Latinoamérica%20presenta%20el,%25)%20y%20ransomware%20(9%25)..

[4] C. Rebollo, «Los ciberataques para secuestrar datos se duplicaron en los seis últimos meses,» El Pais, 18 Agosto 2022. [En línea]. Available: https://elpais.com/tecnologia/2022-08-18/los-ciberataques-para-secuestrar-datos-se-duplicaron-en-los-seis-ultimos-meses.html.

[5] J. A. Bland, M. D. Petty, T. S. Whitaker, K. P. Maxwell y W. A. Cantrell, «Machine Learning Cyberattack and Defense Strategies,» *ELSEVIER,* vol. 92, p. 23, 01 Mayo 2020.

[6] R. V. Roque Hernández y C. M. Juárez Ibarra, «Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios,» *SciELO,* vol. 8, nº 14, 01 Agosto 2018.

[7] L. Mayer Lux y J. Vera Vega, «El delito de espionaje informático: Concepto y delimitación,» *ScieELO,* vol. 9, nº 2, p. 37, 2020.

[8] A. T. Norman, «Hacker types, motivations and strategies: A comprehensive framework,» *ELSEVIER,* vol. 5, p. 100167, 01 Marzo 2022.

[9] M. R. Cando Segovia y R. P. Chicaiza Medina, «Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica,» *Dialnet,* vol. 10, nº 1, pp. 17-41, 29 Marzo 2021.

[10] M. Á. Álvarez Roldán y H. F. Montoya Vargas, «Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos,» *SciELO,* vol. 38, nº 2, pp. 279-297, Dieciembre 2020.

[11] J. Qin, M. LI, J. Wang, L. Shi, Y. Kang y W. X. Zheng, «Optimal Denial-of-Service attack energy management against state estimation over an SINR-based network,» *ELSEVIER,* vol. 119, p. 109090, 01 Septiembre 2020.

[12] S. Phetsouvanh, A. Datta y A. Tiu, «On unlinkability and denial of service attacks resilience of whistleblower platforms,» *ELSEVIER,* vol. 118, pp. 438-452, 01 Junio 2021.

[13] O. Yousurf y R. N. Mir, «DDoS attack detection in Internet of Things using recurrent neural network,» *ELSEVIER,* vol. 101, p. 108034, 01 Julio 2022.

[14] A. Bhardwaj, F. Al-Turjman, V. Sapra, M. Kumar y T. Stephan, «Privacy-aware detection framework to mitigate new-age phishing attacks,» *ELSEVIER,* vol. 96, p. 107546, 01 Diciembre 2021.

[15] I. Sreeram y V. P. Kumar Vuppala, «HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm,» *Applied Computing and Informatics,* vol. 15, nº 1, pp. 59-66, 01 Enero 2019.

[16] K. Singh, P. Singh y K. Kumar, «User behavior analytics-based classification of application layer HTTP-GET flood attacks,» *Future Computing and Informatics Journal,* vol. 112, pp. 97-114, 15 Junio 2018.

[17] O. Thorat, N. Parekh y R. Mangrulkar, «TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification,» *ELSEVIER,* vol. 1, nº 2, p. 100048, 01 Noviembre 2021.

[18] B. Bouyeddou, B. Kadri, F. Harrou y Y. Sun, «DDOS-attacks detection using an efficient measurement-based statistical mechanism,» *ELSEVIER,* vol. 23, nº 4, pp. 870-878, 01 Agosto 2020.

[19] R. K. Batchu y H. Seetha, «An integrated approach explaining the detection of distributed denial of service attacks,» *ELSEVIER,* vol. 216, p. 109269, 24 Octubre 2022.

[20] L. Erdődi, Å. Å. Sommervoll y F. M. Zennaro, «Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents,» *ELSEVIER,* vol. 61, p. 102903, 01 Septiembre 2021.

[21] M. P. Rodríguez Márquez, «Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano,» *Redalyc,* vol. 20, nº 3, p. 28, 10 Mayo 2021.

[22] A. Valenza, L. Demetrio, G. Costa y G. Lagorio, «WAF-A-MoLE: An adversarial tool for assessing ML-based WAFs,» *ELSEVIER,* vol. 11, p. 100367, 01 Enero 2020.

[23] J. M. Domingues y N. F. Ebecken, «A new WAF architecture with machine learning for resource-efficient use,» *ELSEVIER,* vol. 106, p. 102290, 01 Julio 2021.

[24] J. E. Martínez Lozano y P. S. Atencio Ortiz, «CREACIÓN DE UN ATAQUE DDOS UTILIZANDO HTTP-GET FLOOD A PARTIR DE LA METODOLOGÍA CYBER KILL CHAIN,» *Dialnet,* vol. 16, nº 1, pp. 41-47, Junio 2019.

[25] A. Dimitriadis, N. Ivezic, B. Kulvatunyou y L. Mavridis, «D4I - Digital forensics framework for reviewing and investigating cyber attacks,» *ELSEVIER,* vol. 5, p. 100015, 01 Marzo 2020.

[26] K. Razikin y B. Soewito, «Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework,» *Egyptian Informatics Journal,* p. 22, 16 Marzo 2022.

[27] J. N. Al-Laraki, A. Gawanmeh y S. El-Yassami, «GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking,» *Journal of King Saud University - Computer and Information Sciences,* vol. 34, nº 6, Part A, pp. 3079-3095, 01

Junio 2022.

[28] M. Malinova, S. Gross y J. Mendling, «A study into the contingencies of process improvement methods,» *ELSEVIER,* vol. 104, p. 101880, 01 Febrero 2022.

[29] A. Postigo Palacios, Seguridad informática (Edición 2020), Madrid - España: Editorial Paraninfo, 2020, p. 334.

[30] R. A. Proaño Escalante y A. F. Gavilanes Molina, «Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana,» *SciELO,* vol. 9, nº 1, pp. 90-101, Marzo 2018.

[31] S. Bustamante García, I. E. Cuellar Rodríguez, D. Lévano Rodríguez y M. Á. Valles Coral, «Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú,» *Enfoque UTE,* vol. 12, nº 2, pp. 69-79, Junio 2021.

[32] D. Freet y R. Agrawal, «A virtual machine platform and methodology for network data analysis with IDS and security visualization,» Marzo 2017. [En línea]. Available: https://www.researchgate.net/publication/316899449_A_virtual_machine_platform_and_methodology_for_network_data_analysis_with_IDS_and_security_visualization.

[33] D. Kelly, F. G. Glavin y E. Barret, «Denial of wallet—Defining a looming threat to serverless computing,» *ELSEVIER,* vol. 60, p. 102843, 01 Agosto 2021.

[34] D. Canavese, L. Regano, C. Basile, G. Ciravegna y A. Lioy, «Encryption-agnostic classifiers of traffic originators and their application to anomaly detection,» *ELSEVIER,* vol. 97, p. 107621, 01 Enero 2022.

[35] Management Association, Information Resources, Research Anthology on Combating Denial-of-Service Attacks, USA: IGI Global, 2020, p. 655.

ANEXOS

Anexo 1: Encuesta a especialistas

EVALUACION DEL PLAN DE CONTINGENCIA

- **Pregunta 1:** ¿Cree usted que el plan de contingencia elaborado cubre los riesgos más relevantes del servidor y sitio web?

  Totalmente de acuerdo ( ) En desacuerdo ( )
  De acuerdo ( ) Totalmente en desacuerdo ( )

- **Pregunta 2:** ¿Cree usted que la exclusión de direcciones IP es una solución viable en cuanto a ataques de denegación de servicios?

  Totalmente de acuerdo ( ) En desacuerdo ( )
  De acuerdo ( ) Totalmente en desacuerdo ( )

- **Pregunta 3:** ¿Crees usted que el impacto asignado para cada uno de los riesgos solventados por el plan de contingencia está bien determinado?

  Totalmente de acuerdo ( ) En desacuerdo ( )
  De acuerdo ( ) Totalmente en desacuerdo ( )

- **Pregunta 4:** ¿Cree usted que el mantenimiento periódico del servidor ayudara a reducir en gran medida los ataques a este?

  Totalmente de acuerdo ( ) En desacuerdo ( )
  De acuerdo ( ) Totalmente en desacuerdo ( )

- **Pregunta 5:** ¿En qué nivel de seguridad sitúa la información manejada por el servidor de la página web?

  Muy mala ( ) Alta ( ) Media ( ) Baja ( )