DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA ENTIDAD HIPOTÉTICA; SEGÚN VULNERABILIDADES IDENTIFICADAS EN AMBIENTES DE PRUEBAS CONTROLADOS

CARLOS ALBERTO DÍAZ CARMONA
LUIS MANUEL HERRERA LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA, COLOMBIA
2020

DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA ENTIDAD HIPOTÉTICA; SEGÚN VULNERABILIDADES IDENTIFICADAS EN AMBIENTES DE PRUEBAS CONTROLADOS

CARLOS ALBERTO DÍAZ CARMONA
LUIS MANUEL HERRERA LÓPEZ

PROYECTO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor
DANIEL FELIPE PALOMO LUNA
Especialista

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA, COLOMBIA
2020

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia para optar al título de Especialista en Seguridad Informática.

_____

Jurado

_____

Jurado

Barranquilla, día de mes de 2020

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

RESUMEN

El servidor web de una entidad hipotética ha sido víctima de ataques *Defacement* y *Eternal Blue* por parte de *Black Hackers*, en las sedes ubicadas en las ciudades de Bogotá y Cali respectivamente. Dado esto y al proceso de expansión que inician en el presente año, la alta dirección ha decidido contratar a un experto en seguridad informática con el fin de realizar las pruebas de vulnerabilidad que ayuden a descifrar el método de intrusión utilizado, y cada uno de los pasos que siguieron para lograrlo. Para ello se utilizarán herramientas de análisis de seguridad como los *Nmap*, *Metasploit* y *OpenVas* encontradas en la distribución Kali Linux. Al final del análisis se entregará un informe detallado del procedimiento llevado a cabo y de un Plan Estratégico de Seguridad de la Información a implementar en la organización con el fin de solventar los problemas de seguridad en los sistemas de información y prevenir problemas futuros, con el fin de garantizar la seguridad en la prestación de los servicios a sus clientes.

Palabras clave: **Vulnerabilidad, riesgos, seguridad, Plan Estratégico, amenazas, normativas, ataques, ambiente de pruebas, PESI.**

INTRODUCCIÓN

La masificación de los sistemas de información y el aumento de las conexiones de usuarios en internet ha conllevado a elevar la importancia de los temas referentes a la seguridad informática.

Garantizar la seguridad de la información se ha convertido en prioridad para las organizaciones, ya que los atacantes están a la orden del día, al acecho esperando cualquier oportunidad para tomar partido de estas y explotar las vulnerabilidades detectadas en los sistemas, derivando en la necesidad de que cada día surjan un mayor tipo de soluciones relacionadas con ciber seguridad.

En el desarrollo de este trabajo se utilizan distintas técnicas de explotación de vulnerabilidades, así como herramientas relacionadas con pruebas de penetración que ayudarán a comprobar la importancia de tener sistemas seguros a partir de prácticas realizadas en ambientes de prueba.

Colombia ocupa actualmente a nivel mundial el puesto número 24 como objetivo de ataques informáticos, de allí la importancia de la utilización de técnicas capaces de garantizar sistemas informáticos seguros. (Asosec, 2018)

Normas como la ISO 27000 brindan una guía de la manera como se debe desarrollar y como evitar vulnerabilidades en las implementaciones, no solo a nivel lógico sino también a nivel físico. Se deben evaluar cada uno de los aspectos que pueden hacer vulnerable un sistema, donde cada decisión tomada es importante y donde tiene relevancia la realización de un análisis de las amenazas frente a riesgos y el diseño de un plan que permita la implementación de diferentes proyectos de seguridad que permitan salvaguardar los sistemas de información de una organización.

1. PLANTEAMIENTO DEL PROBLEMA

Una organización hipotética ha sido víctima de ataques informáticos por parte de *black hackers*, los cuales utilizaron ataques de *Defacement* y *Eternal Blue*. Estos ataques afectaron el funcionamiento del servidor web de la ciudad de Bogotá y el servidor de la ciudad de Cali, viéndose comprometida la confidencialidad de las contraseñas y de la información de los usuarios almacenada en la base de datos. Adicionalmente, dado al proceso de expansión que inicia este año, la alta dirección se encuentra preocupada por la seguridad de la información y de los sistemas que maneja la organización y teme que no se entregue un servicio de calidad a sus clientes, lo que puede derivar en la pérdida de sus clientes generando así pérdidas económicas para la organización.

2. JUSTIFICACIÓN

Una organización hipotética ha sido víctima de ataques informáticos por parte de *black hackers*, los cuales utilizaron ataques de *Defacement* y *Eternal Blue*. Estos ataques afectaron el funcionamiento del servidor web de la ciudad de Bogotá y el servidor de la ciudad de Cali, viéndose comprometida la confidencialidad de las contraseñas y de la información de los usuarios almacenada en la base de datos. Adicionalmente, dado al proceso de expansión que inicia este año, la alta dirección se encuentra preocupada por la seguridad de la información y de los sistemas que maneja la organización y teme que no se entregue un servicio de calidad a sus clientes.

El presente trabajo permite demostrar la importancia de la implementación de políticas y controles de seguridad sobre los sistemas de información de una organización, pues a pesar de lo sensible que puede ser el tema de la falta de disponibilidad, confiabilidad e integridad de la información se considera que en muchas organizaciones no se brinda el manejo adecuado a esta situación.

Es importante tener claro que ningún sistema es 100% seguro, por lo cual lo que se busca dentro de una organización es llevar los riesgos a un nivel aceptable definido, de tal forma que se minimice la exposición de los activos de información a las diferentes amenazas que puedan existir.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un plan estratégico de Seguridad de la Información en una organización que permita la aplicación de controles y políticas que garanticen la corrección de vulnerabilidades detectadas a través de diferentes herramientas de seguridad y prevención de diferentes ataques como *Defacement* y *Eternal Blue*.

3.2 OBJETIVOS ESPECÍFICOS

- Configurar un ambiente de pruebas para el análisis de vulnerabilidad y ejecución de ataques *Defacement* y *Eternal Blue*
- Ejecutar los ataques Defacement y *Eternal Blue* en un ambiente controlado de pruebas.
- Realizar el análisis de gestión de riesgos como parte del plan estratégico de Seguridad de la Información.
- Sugerir a partir de los objetivos de la organización, el diseño de un Plan Estratégico de la Seguridad de la Información basado en metodologías de la gestión de riesgos informáticos.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL Y TEÓRICO

Hoy en día parte de las actividades cotidianas dependen del uso de los sistemas informáticos[1], tanto que para que una organización funcione adecuadamente, sus procesos de negocio se optimizan con el uso de herramientas tecnológicas. Dado este crecimiento y su importancia en la actualidad, se debe garantizar la seguridad informática y la seguridad de la información.

Seguridad informática: El término seguro según la Real Academia de la lengua española, es estar libre, apartado de todo daño, amenaza, peligro u obstáculo. Por lo tanto, en lo que respecta a la disciplina de seguridad informática, implica el procedimiento de diseño de normas, técnicas y métodos que faciliten la estructuración de un sistema de información seguro y confiable[2].

Desde esta perspectiva, la seguridad informática es una estructuración de ingeniería, creatividad fundamentada en criterios éticos y valores morales en sus procesos normativos. Con ella se "protege la integridad y privacidad de la información almacenada en un sistema informático de cualquier tipo de amenaza"[3].

Puesto que el universo de los sistemas de información es vulnerable, pues puede sufrir daños, ataques, la pérdida de datos y múltiples siniestros. Es allí donde se hace indispensable para las empresas tener conocimientos de cómo definir y garantizar la seguridad de sus herramientas informáticas[4].

Las empresas sin una adecuada seguridad informática son presa fácil de los ataques, ya que les es fácil a los atacantes buscar y encontrar debilidades en los sistemas abiertos en internet. La vulnerabilidad se evidencia en los servidores web o los servidores de correo electrónico, los cuales vienen a conformar un sistema de frontera como una especie de interfaz entre internet y la red interna. La forma de ataque sobre esta vulnerabilidad progresa desde esta frontera hasta la red interna de la empresa vulnerando las máquinas, controles de dominio, servidores de bandejas de correo electrónico, entre otros.

[1] AGUILERA, Purificación. Seguridad Informática. Madrid: Editorial Editex, S.A, 2010. 9p
[2] Ibíd.
[3] BACA Daniel. Introducción a la Seguridad Informática. México: Grupo Editorial Patria, 2016. 12p.
[4] CARPENTIER Jean-Francois. La seguridad Informática en la PYME: Situación actual y mejores prácticas. Barcelona: Ediciones ENI, 2016. 15p.

Es muy importante para una empresa el proteger, preservar la información y la integridad de su sistema informático, ya que lo contrario implicaría la pérdida de grandes sumas de dinero en su reparación, unida a la pérdida de tiempo e información valiosa. En fin, este conjunto de procedimientos, dispositivos y herramientas se encargarán de asegurar la integridad, disponibilidad y privacidad de la información[5].

Seguridad de la información: La seguridad de la información dejó de ser en la actualidad de uso exclusivo del gobierno en lo que respecta a secretos militares o diplomáticas, a tener una amplia utilización de dimensiones inimaginables entre las que están: transacciones financieras, acuerdos contractuales, información personal, comercio y negocios por internet entre otras aplicaciones. De allí que sea importante que las necesidades de seguridad de la información potencial, en cualquier empresa o entidad sean tenidas en cuenta y se elaboren para todo tipo de aplicaciones[6].

La disciplina de la seguridad de los sistemas de información aún está en continua evolución. El uso de la internet viene a ocupar un lugar imprescindible en la vida de las personas, es un medio a través del cual se ha incrementado la actividad económica a nivel mundial. Es por esta razón, que lo ha llevado a constantes peligros y amenazas globales que tienen gran impacto en la seguridad de la información mundial y nacional. Ningún país se escapa de sufrir las consecuencias de un ataque a sus sistemas informáticos, el cual podría causar un daño devastador en la economía de un estado[7].

Para asegurar la confianza en las redes y los sistemas de información se requiere que los particulares, las empresas y las instituciones públicas estén lo más informados, educados y formados en lo que respecta a la seguridad de las redes y de la información. Las políticas de seguridad eficientes deben estar fundamentados en métodos de evaluación de riesgos bien estructurados, tanto en el sector privado como en el estatal, esto incrementará satisfactoriamente el nivel de seguridad[8].

En todas las organizaciones tanto públicas como privadas, en sus sistemas de información y manejo de datos está en la obligación de definir una estricta política de copias de seguridad, las cuales son duplicados de toda la información o parte de ella, que se debe conservar en algún medio independiente en el que se encuentre normalmente, puesto a que, en el caso de que se borre la información por un fallo

[5] RASCAGNERES Paul. Seguridad Informática y Malwares. Barcelona: Ediciones ENI, 2016. 17p.
[6] ALEGRE, María y GARCÍA, Alfonso. Seguridad Informática Ed.11. España: Paraninfo, 2011. 2p.
[7] AREITIO Javier. 2008. Seguridad de la información: redes, informática y sistemas de información, p. 2. España: PARANINFO.
[8] REVISTA DE LA SEGUNDA CORTE DEL DOCTORADO DE SEGURIDAD ESTRATÉGICA, 2014. Seguridad de la información, p. 31. Guatemala: Universidad San Carlos de Guatemala

accidental en el sistema, si se ha creado la copia de seguridad no presentará ningún problema en restaurarla[9].

Confidencialidad: Es la característica que asegura que los usuarios como: personas, procesos, entre otros, no tengan acceso a los datos salvo que estén autorizados para ello[10].

En el universo de la seguridad de la información, la confidencialidad es la protección de los datos e información que se intercambia en los sistemas[11].

Para el desarrollo de la seguridad informática se parte de las políticas, estándares y procedimientos, controles de riesgos correspondientes tanto físicos como lógicos, la clasificación de la información, la confidencialidad y la integridad, la seguridad de los programas su disponibilidad y continuidad de las operaciones[12].

Sólo a las personas autorizadas se les permite un acceso lógico y una custodia física. La información debe mantenerse bajo llave cuando no está en uso[13].

Integridad: Cuando se diseña una Base de Datos en un Sistema informático específico y se escribe el esquema, no solamente se definen las estructuras de los datos, sino que es de suma importancia establecer las reglas de integridad de la Seguridad de la Base de Datos que se debe hacer cumplir. Existen dos reglas fundamentales de integridad: las del usuario, las cuales son reglas propias de la realidad que intenta representar las bases de datos que se quieren crear. La segunda son las reglas de integridad adheridas al modelo de datos utilizado en el sistema gestor de bases de datos[14].

Existe diferencia entre la integridad de una unidad de datos y la integridad de la secuencia de unidades de datos. Al elaborar la integridad de una unidad de datos la entidad emisora integra una cantidad de reglas encriptadas con técnicas simétricas o asimétricas en función de los datos, la cual es una información suplementaria compuesta por códigos de control de bloqueos o un valor de control criptográfico. En la elaboración de la integridad de la secuencia de datos es

[9] GONZÁLEZ L. 2008. La sociedad de la información en Europa, p. 183. Madrid: Editorial REUS S.A.
[10] AGUILERA P. 2011. Políticas de almacenamiento y resguardo de la información, p.194. Madrid: Editex.
[11] PACHECO F. y Jara H. 2012. Hackers al descubierto: advierta sus vulnerabilidades evite que lo sorprendan, p.19. Argentina: USERS
[12] PEQUEÑO M. 2015. MF0490_3. Gestión de servicio en sistema informático, p.380. España: Editorial ELEARLING S.L
[13] DEL PESO E. 2003. Manual de outsourcing informático. España: Ediciones Diaz de Santos.h76
[14] FISHER R. 1988. Seguridad en los sistemas informáticos, p. 178. Madrid: Ediciones Diaz de Santos

imprescindible una ordenación explicita como: un ordenamiento criptográfico, la numeración de secuencias o un sello de tiempo[15].

La integridad y disponibilidad de los datos es el bien jurídico de una entidad pública o privada, que está protegido esencialmente en algunas de las figuras del delito relacionadas con la informática, la cual se comprende como la incolumidad de los datos, su libre disposición y mantenimiento en el término que los ha configurado su dueño. Cuyo bien jurídico apunta a la tutela de los datos en sí mismos como objeto de la protección penal[16].

Disponibilidad: Toda información debe estar disponible para los usuarios autorizados, esto se define como: "grado en el que un dato está en el momento, lugar y forma como es solicitado por el usuario autorizado", es cuando se accede a un sistema de información en periodo de tiempo aceptable. Esta disponibilidad se asocia a los sistemas de fiabilidad técnica de los componentes del sistema de información[17].

La disponibilidad asegura que los recursos del sistema y la información pueda ser accedida en cualquier momento solamente por los usuarios que tengan los permisos para acceder[18].

Se disponen de varias copias de algunos archivos y cada una de ellas se encuentra en un servidor de archivos independiente. La razón esencial de este procedimiento informático radica en que busca mejorar la confiabilidad y la disponibilidad, al disponer de respaldos independientes de cada archivo[19].

Autenticidad: En el entorno de las redes y las comunicaciones, una variación de integridad es la autenticidad, la cual, facilita los medios para que se verifique de donde provienen los datos y si es correcta su procedencia, ¿quién los envía? ¿cuándo fueron enviados y recibidos? Tanto en el mundo financiero y

[15] MARCO María Jesús y Marco José María, 2010. Escaneando la informática, p.152. Barcelona: Editorial UOC.
[16] ECHEVERRÍA Guido, 2012. Procedimientos y medidas de seguridad informática, p.165.
[17] GONZÁLEZ Juan José, De la Mata Norberto, Morón Esther… Adán Carmen, 2007. Delito e informática algunos aspectos, p.17. Bilbao: Universidad de DEUSTO.
[18] AGUILERA Purificación, 2010. Seguridad Informática, p. 11. Madrid: Editorial Editex, S.A.
[19] PACHECO F. y Jara H. 2012. Hackers al descubierto: advierta sus vulnerabilidades evite que lo sorprendan, p.19. Argentina: USERS.

gubernamental, este aspecto de la seguridad informática es supremamente importante[20].

La autenticidad implica que se puede confirmar que el mensaje recibido haya sido enviado por quien asegura que lo envió y que este mensaje sea el que el receptor estaba esperando. La criptografía asimétrica es la técnica más usada para verificar la autenticidad de un dato o mensaje, esta consiste en la firma digital, que de alguna forma sustituye la firma autógrafa común[21].

Los mecanismos de protección deben garantizar la integridad, secreto y autenticidad del trayecto en dos importantes estados del móvil: en el tránsito o migración ejecutados en una plataforma, en la migración el trayecto no puede ser manipula ni accedido ni su origen falsificado. De esta forma, las aplicaciones fundamentadas en móviles son adecuadas en contextos donde existe una fuerte competencia entre plataformas con lealtad a los usuarios[22].

No repudio: Los servicios de no repudio brindan a los usuarios involucrados en intercambios electrónicos de datos, amparo contra cualquier usuario que niegue que realizó transferencia o entrega de información en el lugar o memento en que se produjo. Aun cuando estos servicios pueden impedir que un usuario niegue la existencia de un suceso, aseguran la disponibilidad de evidencias irrefutables para solucionar rápida y justamente la controversia entre emisores y receptores[23].

No repudio de Origen, es imposible que el emisor niegue su envío, puesto a que el destinatario tendrá las pruebas de lo enviado, él recibe una prueba infalsificable del origen del envío. Por otra parte, el no repudio de destino, no puede negar el receptor que recibió el mensaje, puesto a que el emisor tiene la evidencia de haberlo enviado. Este servicio le brinda al emisor la prueba de que el destinatario legítimo lo recibió[24].

Los servicios de no repudio se utilizan fundamentalmente en los sistemas de transmisión de mensajes y el comercio electrónico. Sus protocolos generan

---

[20] ORJUELA, Juan. Diseño de una arquitectura web distribuida de alta disponibilidad para sistemas de educación a distancia por medio de Oracle WebLogic Server. [En línea]. Juan Jose Orjuela castillo. Disponible en https://books.google.com.co/books?id=eyq7BgAAQBAJ

[21] SÁNCHEZ José Salvador, Chalmeta Ricardo, Óscar Coltell, Monfort Pilar y Campo Cristina.2003. ingeniería de proyectos informáticos: actividades y procedimientos, p.103. España: Universidad de Jaume

[22] GARCÍA Héctor, 2006. Avances en informática y sistemas computacionales (CONAIS 2006), p. 122. México: Universidad Juárez Autónoma de Tabasco).

[23] Ramos Benjamín y Ribagorda Arturo, 2004. Avances en criptología y seguridad de la información, p. 353. Madrid: Diaz de Santos.

[24] AREITIO Javier. 2008. Seguridad de la información: redes, informática y sistemas de información, p. 384. España: Paraninfo.

evidencias que garantizan los servicios de no repudio, en caso de discordias, un juez, evalúa las evidencias y toma una decisión a favor de una de las partes[25].

Amenaza: La amenaza es un acontecimiento que produce incidentes en una empresa u organización, ocasionando daños materiales o pérdidas de sus activos intangibles. Su naturaleza potencial es una acción, interrupción o falta de acción ubicada lejos del control de los encargados de la seguridad. Las consecuencias de las amenazas si se materializan, modificarán el estado de seguridad de los activos amenazados. Por lo tanto, existen multiplicidad de consecuencias, por lo hay que tener en cuenta al analizar la entidad del impacto, de igual manera existen cuatro causas específicas de amenazas estas son: no humanas o accidentes, humanas pero involuntarias o errores, intencionales humanas con presencia física y humanas intencionales de procedencia remota[26].

Las amenazas más frecuentes son:

- Usuarios: Ciertas acciones realizadas por algunos usuarios pueden resultar dañinas dado que tienen permisos sobre dimensionados y no se les restringe de acciones innecesarias.
- Programas maliciosos: están destinados a perjudicar y hacen uso ilícito de los recursos del sistema. Son instalados por maldad o falta de atención en el ordenador, un sistema operativo, un programa o un sistema de operación, el cual abre puertas a los intrusos o modifica los datos.
- Virus informático: es un programa malicioso cuyo objetivo es alterar el buen funcionamiento del ordenador, sin permiso o conocimiento del usuario. Normalmente sustituyen los archivos ejecutables por otros infectados con el código de él. Ellos pueden eliminar de forma intencionada, datos almacenados en la computadora.
- Gusano informático: es un programa malicioso, que tiene la propiedad de multiplicarse a sí mismo. Se ubica en las partes de un sistema operativo y son invisibles para el usuario, se propagan de ordenador a ordenador, sin embargo, son diferentes a un virus, porque se propagan sin la ayuda de una persona, lo más letal de ellos es esa capacidad de multiplicarse en el sistema.
- El troyano: es un programa malicioso, que se presenta aparentemente inofensivo ante el usuario, que al ejecutarlo realiza un fuerte ataque remoto al equipo.
- Programa espía o *spyware*: recopila información de un ordenador y luego la transmite a una entidad externa sin el conocimiento y consentimiento del dueño. Este término también es utilizado para referirse a otros productos que no son espías, los cuales realizan las funciones de mostrar anuncios no solicitados (*pop up*), recopilar información privada, redireccionar solicitudes de páginas e instalar marcadores de teléfonos.

[25] TERÁN David, 2014. Administración estratégica de la función informática. México: ALFAOMEGA
[26] RAMOS Benjamín y Ribagorda Arturo, 2004. Avances en criptología y seguridad de la información, p. 279. Madrid: Diaz Santos.

- Error de programación: la mayoría de ellos son una amenaza informática por causas intencionales, también se dan casos en las que el desarrollo es, en sí mismo, una amenaza. Lo que permite contrarrestar este tipo de amenazas es la actualización de parches de los sistemas operativos.
- Intrusos: personas que acceden a los datos o programas sin autorización (*Crackers*, *Hackers*, *script kiddie* o *script boy*, entre otros)[27].

Ataque: cuando se quiere llevar a cabo un ataque informático, el intruso debe disponer de los medios técnicos, conocimientos y herramientas adecuadas, contar con una determinada motivación o finalidad y contar con una determinada oportunidad que le facilite el ataque. Los ataques contra ordenadores y sistemas informáticos constan de las siguientes etapas a saber:

- Descubrimiento y exploración del sistema.
- Indagación sobre las vulnerabilidades del sistema.
- Explotación de las vulnerabilidades detectadas con herramientas "*exploits*".
- Corrupción o compromiso del sistema.
- Eliminación de pruebas que revelen el ataque y compromiso del sistema[28].

La persona no autorizada que desea obtener información emplea algún tipo de ataque informático, estos ataques se dividen en dos grupos a saber: ataques pasivos y ataques activos.

Los pasivos son:

- Espionaje o *Surveillance:* se observa el entorno y se recopila la información de la tipología de la red. Para ser empleada en sucesivos ataques.
- Escuchas o *sniffing*: el objetivo es monitorearla red para captar información, paso previo de ataques posteriores (MAC o IP) origen y destino.
- Ataques de contraseñas: se utiliza la contraseña de un usuario autorizado para descifrar códigos encriptados.

[27] MOLINER López Francisco Javier, 2005. Informáticos de la generalitat valenciana grupos A y B. bloque específico, temario volumen II, p. 203. España: Editorial MAD.
[28] EDITORIAL CEP, 2017. Cuerpo auxiliar (C2). Junta de comunidades de Castilla. La Mancha. Temario. p. 32. Madrid: Editorial CEP.

Los ataques activos, modifican el flujo de datos o se crean flujos falsos en la transmisión de datos, estos son los ataques:

- Ataque de denegación de servicios: consiste en colapsar total o parcialmente un servidor para que este no pueda realizar su tarea, se inunda el servidor con una gran cantidad de solicitudes para saturarlo. Ejecutado a través de una red zombis.
- *Phishing*: Es un tipo de ataque que se utiliza para engañar a la víctima a través del envío de correos electrónicos o falsificación de sitios web, con el fin de solicitarle información personal.
- *Spam*: mensajes de todo tipo que no han sido solicitados por el usuario.
- *Spoofing*: suplanta validaciones, credenciales e identificadores estáticos.
- *Man in the Middle*: basado en *spoofing* que se interpone entre dos sistemas. Intercepta y selectivamente modifica los datos de la comunicación para suplantar la identidad de los usuarios.
- Secuestro de sesiones o *hijacking*: usa el *spoofing* para robar la sesión entre dos usuarios al tomar la conexión existente.
- Código malicioso: se introduce en un sistema con un fin malicioso y no autorizado *(hardware, software, firmware*).
- *Hoax*: es un falso mensaje de correo electrónico distribuido en cadena, que congestiona las redes y los servidores de correo[29].

Según la motivación y el interés de un ataque informático es lo que lo puede convertir en un delito penal, esto si es verdaderamente serio. Si la gravedad del ataque afecta la seguridad de una nación o es a nivel internacional será tratado por una jurisdicción penal a través de la Corte Penal Internacional[30].

***Defacement*:** Es cuando el atacante accede y lleva a cabo el segundo de los ataques más típicos de internet, el *defacement* o desfiguración, suplanta el contenido real del sitio atacado por uno que instalan los *hackers*, el cual es reivindicativo[31].

Es la manipulación del programa, causando alteraciones de las instrucciones con que ha sido diseñado en su configuración original, con el fin de que actúe de forma

[29] GÓMEZ Álvaro, 2017. Enciclopedia de la seguridad informática. 2° edición. España: Ra-Ma.
[30] VALDIVIA Carlos, 2017. Informática industrial, p. 84. Madrid: Paraninfo.
[31] AMBOS KAI, 2015. Responsabilidad penal internacional en el ciberespacio, p. 13. Colombia: Universidad Externado de Colombia.

diferente, logrando de esta forma la desfiguración de los datos correctamente introducidos[32].

***Eternal Blue*:** Estos *exploits* son utilizados por cualquier pirata informático que desee aprovecharse de las vulnerabilidades de un sistema informático, por su naturaleza no necesita del usuario para infestar, ya que llega simplemente a través de la red y se propaga automáticamente a otros ordenadores, para protegernos esta peligrosa amenaza se hace necesario, instalar los parches de seguridad que corrigen estos problemas[33].

Eternal Blue es la vulnerabilidad que ha hecho tan letales estas últimas campañas de *ramsonware*: a través de este agujero de seguridad en Windows, hasta el virus más simple tiene la capacidad de infectar en cuestión de segundos a todos los ordenadores que estén conectados a una misma red. Dado que existe mucha confusión acerca de qué versiones de Windows están protegidas ante esta amenaza (lo están hasta las más antiguas), la herramienta de Eternal Blues es ideal para todo aquel que quiera asegurar que en su red no hay ningún equipo vulnerable a uno de estos ataques[34].

Eternal Blues es una aplicación gratuita que, con un solo clic, permite comprobar si un ordenador, o cualquier otro conectado a la red local, es vulnerable ante Eternal Blue y se puede llegar a ser víctimas de los piratas informáticos o, de lo contrario, los ordenadores están protegidos y no hay peligro de infectarlos con estas vulnerabilidades. La herramienta es muy útil tenerla a la mano, sobre todo en entornos corporativos donde los sistemas son más heterogéneos[35].

Riesgo: el riesgo informático, es un nuevo concepto en la terminología jurídica, el cual no tiene una definición específica. Sin embargo, este refiere a la incertidumbre

---

[32] CASAS, Eduardo. La red oscura: En las sombras de Internet: el cibermiedo y la persecución de los delitos tecnológicos. [En línea]. Madrid: La Esfera de los Libros. Disponible en https://books.google.com.co/books?id=GonFDQAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[33] VARIOS AUTORES, 2017. Policía Nacional Escala Ejecutiva Inspector: volumen III, p. 54. Madrid: Editorial CEP.

[34] VELASCO, Rubén. Comprueba si eres vulnerable al exploit EternalBlue con Eternal Blues. [En línea]. Disponible en https://www.softzone.es/2017/06/30/comprobar-vulnerabilidad-eternalblue

[35] MOTYKA, Jakub. Esta herramienta te dice si tienes un PC vulnerable a Eternal Blue. [En línea]. Disponible en https://computerhoy.com/noticias/software/esta-herramienta-te-dice-si-tienes-pc-vulnerable-eternal-blue-64460

o probabilidad de que ocurra o se realice una amenaza o daño a bienes y servicios informáticos[36].

Riesgos físicos y riesgos lógicos, son los dos tipos de riesgos a los que se exponen los sistemas de información y de cuya minimización está a cargo de la seguridad informática:

- Riesgos Lógicos: son muy peligrosos y difíciles de detectar están asociados a la tecnología de los propios sistemas de información y afectan directamente el *software*. Las alteraciones que se le hacen al funcionamiento del sistema le ocasionan daños irreparables, se realizan con códigos maliciosos.
- Riesgos físicos: son aquellos que afectan la continuidad de los procesos de negocios de una organización al afectar la disponibilidad de la información su activo más preciado[37].

Las mínimas medidas de seguridad que deben realizarse para generar la confianza del usuario son:

- El análisis de los riesgos de cualquier tipo de sistemas de información o de sus elementos, observando y conjuntando las estimaciones de su vulnerabilidad ante las amenazas y el impacto o daño que una mala seguridad puede tener la organización.
- A partir de la gestión de los riesgos, con base en el análisis, se deben seleccionar las medidas de seguridad adecuadas para conocer, prevenir, impedir, reducir y controlar los riesgos identificados[38].

DMZ: Es un ambiente de subred ubicado entre una red interna de confianza y una red externa no segura. Los servidores instalados en la parte externa de la DMZ ofrecen servicios a la red externa, estos pueden ser:

- Servidores web, de archivos, de correo y servidores de nombres.

[36] ALEJANDRO. Utilidad para testear la vulnerabilidad a Eternal Blue. [En línea]. Disponible en https://protegermipc.net/2017/07/03/utilidad-para-testear-la-vulnerabilidad-a-eternalblue
[37] TÉLLEZ Julio, 1988. Contratos, riesgos y seguros informáticos, p. 33. México: Universidad Nacional Autónoma de México.
[38] PEQUEÑO María Victoria, 2015. MF0490_3-Gestión de servicio en sistema informático, p. 56. España: Editorial ELEARLING.

- Servidores de relevo que permiten garantizar una comunicación indirecta entre la red local y la red de internet[39]

De esta forma, los equipos de una red perimetral o zona desmilitarizada proporcionan servicios a la red externa y lo hace para proteger a la red interna, ya que por su configuración cualquier intruso ataca primero a la DMZ y no se le permite el ingreso a la red interna[40].

Vulnerabilidad: es la debilidad de un sistema informático, que es aprovechada por intrusos para ocasionar pérdidas o daños. Existe una analogía muy clara en cierta terminología de la seguridad informática, en el sentido de que una exposición es análoga a un accidente y vulnerabilidad es análoga a una contingencia[41].

La vulnerabilidad de un sistema informático es la probabilidad de que una amenaza se materialice sobre un activo. Para investigarla debe estar a cargo un profesional que conozca profundamente los activos del sistema de información y las amenazas y riesgos que pueden sufrir.

Las siguientes son tres tipos de vulnerabilidades:

- Vulnerabilidad intrínseca, proviene directa y exclusivamente del activo y de la amenaza.
- Vulnerabilidad efectiva, se ha originado a partir de una salvaguarda ya existente en el sistema de información.
- Vulnerabilidad residual, se genera por la aplicación de salvaguardas implantadas siguiendo el resultado del proceso de análisis y gestión de riesgos[42].

[39] CARVAJAL Francisco, 2017. Gestión de servicios en el sistema informático, p. 88. Madrid: Editorial CEP.

[40] CARPENTIER Jean-Francois, 2016. La seguridad informática en la PYME: situación actual y mejores prácticas, p. 89. Barcelona: Ediciones ENI.

[41] BACA Gabriel, 2016. Introducción a la seguridad informática, p. 209. México: Grupo Editorial Patria.

[42] SOMMERVILLE Iam, 2005. Ingeniería del software, séptima edición, p.54. Madrid: PEARSON.

Cuando se detecta una vulnerabilidad nueva se crea un filtro específico y se añade al sistema de prevención de intrusos (*IPS*, por sus siglas en inglés), de modo que cualquier intento malicioso se bloquee de forma automática[43].

***Firewall*:** Es un sistema de defensa basado en el hecho de que todo tráfico de entrada o salida en la red debe pasar obligatoriamente por el sistema de seguridad que sea capaz de autorizar, denegar y tomar nota de todo lo que sucede, acorde con las políticas de acceso entre redes.

El *firewall* no es solo un programa, es un conjunto de medidas *hardware* y *software* destinadas a asegurar las instalaciones de la red[44].

Un *firewall* es una parte de un sistema o una red que se diseñó para bloquear el acceso no autorizado de intrusos y permite al mismo tiempo las comunicaciones que se han autorizado[45].

El *firewall* tiene limitaciones, es simplemente un filtro que atraviesa la información cuando transita a partir de redes o la computadora personal, de allí que las amenazas se mantienen vigentes si estos ataques traspasan el firewall, puesto que el filtrado de la información no es estricto. Un firewall tampoco puede proteger de ataques internos a una organización o de las amenazas ocasionadas por usuarios descuidados y negligentes[46].

Kali Linux: Es una distribución derivada de Debian, que se especializa en pruebas de penetración. Provee *software* para auditar la seguridad de una red o equipo en el que se ejecuta, y analiza resultados después del ataque, también conocido como informática forense[47].

LiveCD Linux ha adquirido gran fama y respeto en el mundo de la seguridad informática, la distribución Kali que sucede a *Backtrack*. Puede ejecutarse o instalarse desde un *liveCD*. Engloba múltiples utilidades de *pentesting* para auditar

[43] CHICANO Esther, 2014. MF0487_3: Auditoría de seguridad informática. Málaga: IC Editorial.
[44] CHICANO Esther, 2014. Gestión de servicios en el sistema informático. IFCT0509. Málaga: IC Editorial.
[45] VARIOS AUTORES, 2016. Técnicos especialistas en radiodiagnósticos: servicio andaluz de salud (SAS), p. 358. Madrid: Editorial CEP.
[46] CARVAJAL Francisco, 2017. Gestión de servicios en el sistema informático, p. 73. Madrid: Editorial CEP.
[47] BACA Gabriel, 2016. Introducción a la seguridad informática, p. 218. México: Universidad Autónoma).

sistemas informáticos y contiene lo necesario para obtener bases de datos de usuarios *Windows*[48].

OWASP: Es una organización sin ánimo de lucro y no está afiliada a ninguna compañía de tecnología, está en una posición única para facilitar información imparcial y práctica sobre *AppSec* (Seguridad en Aplicaciones) a personas, corporaciones, universidades, agencias gubernamentales y otras organizaciones en todo el mundo. Publica herramientas de software y documentación basada en el conocimiento sobre la seguridad de las aplicaciones[49].

Las recomendaciones del proyecto *OWASP*, para evaluar la seguridad de las aplicaciones *web*, así como en la guía de pruebas de seguridad de red. Se identifican las vulnerabilidades y se utiliza el estándar CVE, el cual se encarga de asignar un identificador único a cada vulnerabilidad publicada, facilitando su seguimiento y control[50].

Según la *Open Web Application Security Project* (OWASP, Proyecto abierto de seguridad en aplicaciones web), los principales problemas de seguridad relacionados con aplicaciones internas son:

- Almacenamiento de datos no seguro
- Controles débiles del lado de los servidores
- Falta de protecciones correctas en las capas de la red
- Autenticación y protección de accesos erróneas
- Inicio de sesión incorrectos
- Problemas de cifrado[51].

4.2 MARCO LEGAL

El gran auge de la tecnología y su aplicación masiva en los sistemas de información, conllevó desafortunadamente al incremento en la realización de ilícitos, por tal motivo a partir del año 2009 el estado colombiano realiza una modificación al código penal y se crea un nuevo bien jurídico el cual se denomina “de la protección de la

[48] VARIOS AUTORES, 2015. Seguridad informática Hacking ético, p. 201. Barcelona: Ediciones ENI.
[49] ZU, Jhonatan. ¿QUE ES EL PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB (OWASP)? [En línea]. Disponible en http://seguridadaguijon.blogspot.com/2018/03/que-es-owasp.html
[50] GÓMEZ Álvaro, 2017. Enciclopedia de la seguridad informática. 2° edición. España: Ra-Ma.
[51] CARPENTIER Jean-Francois, 2016. La seguridad informática en la PYME: situación actual y mejores prácticas, p. 195. Barcelona: Ediciones ENI.

información y de los datos” en esta se habla de la preservación de los sistemas que utilicen las tecnologías de la información y las comunicaciones, así como también se tipifican las sanciones que pueden incurrir quienes atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas de información.

Como complemento a lo anterior en el año 2012 surge la ley de protección de datos personales

A continuación, se listan las dos leyes vigentes en el estado colombiano relacionadas con la protección de datos:

- Ley 1273 de 2009: Esta ley está enfocada en la protección de la información y de los datos, describiendo los delitos informáticos que fueron incluidos en el código penal de Colombia

- Ley 1581 de 2012: Esta ley constituye el marco general de la protección de datos personales en Colombia.

5. DISEÑO METODOLÓGICO

Para la realización del primer ataque, *Defacement*, se realiza la instalación y configuración de una máquina virtual en VirtualBox con sistema operativo *Metasploitable* 2, el cual simulará ser el sistema atacado de la registraduría. Esta máquina virtual se configura en una red NAT.

Posteriormente, se realiza la instalación y configuración de una máquina virtual en VirtualBox con el sistema operativo Kali Linux, desde la cual se lleva a cabo el ataque al sistema *Metasploitable* 2. Esta máquina virtual se configura en una red NAT. Durante la preparación del entorno, primero se realiza la actualización de Kali Linux.

Para escanear las vulnerabilidades del sistema *Metasploitable*, se utilizan las herramientas *Nmap* que viene instalada en el sistema operativo Kali Linux y *OpenVas*, la cual se debe instalar para realizar el escaneo.

Una de las vulnerabilidades en el sistema *Metasploitable*, es a un ataque CGI. Se utiliza el *Mestasploit* Framework para encontrar y utilizar un *exploit* que permita materializar la vulnerabilidad encontrada.

Para realizar el segundo ataque, *Eternal Blue*, se realiza la instalación sobre una máquina virtual en el programa *Virtual Box* del sistema operativo Windows 7, este no cuenta con las ultimas actualizaciones, lo cual es un caso muy común, además de que el *firewall* no cuenta con la configuración correcta. Esta máquina también se configura en una red NAT.

Se realiza un escaneo de las vulnerabilidades del sistema con Windows 7 y posteriormente se procede a utilizar el *Mestasploit Framework* para encontrar y utilizar un *exploit* que permita explotar la vulnerabilidad en el servicio SMB.

Durante la realización de cada una de las actividades anteriores, se realizan consultas en internet para conocer los comandos a utilizar. Adicionalmente, Durante el desarrollo de los análisis se registrará el paso a paso de los procedimientos realizados con registros de capturas de pantalla utilizando los lineamientos establecidos por la norma NTC 1486.

El tipo de investigación a utilizar es aplicado, dado que se busca dar respuesta a interrogantes puntuales acerca de un problema conocido. Las técnicas de recolección de datos que se utilizarán en el proyecto son la observación y entrevistas.

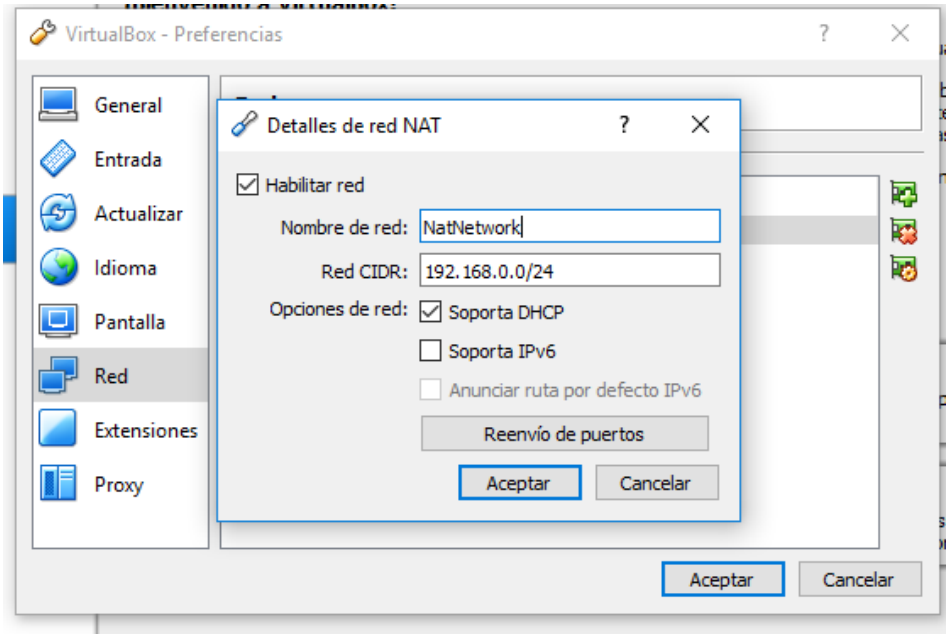
6. AMBIENTES DE PRUEBA

6.1 CONFIGURACIÓN DE LOS AMBIENTES DE PRUEBAS

Par iniciar los análisis de vulnerabilidad se realiza la configuración de redes NAT en las máquinas virtuales instaladas bajo el sistema operativo Windows 10. A continuación, se presenta la documentación de dicho proceso.

Una vez se cuenta con las máquinas virtuales debidamente instaladas y configuradas con los sistemas operativos Linux *Metasploitable, Windows 7 y Kali Linux,* se procede a ejecutar VirtualBox, una vez hecho esto se debe proceder a la configuración de la red para ello se debe dirigir a la pestaña archivo, dar clic sobre ella, luego clic en preferencias, y en la ventana desplegada se ingresará la dirección IP de la red a configurar.

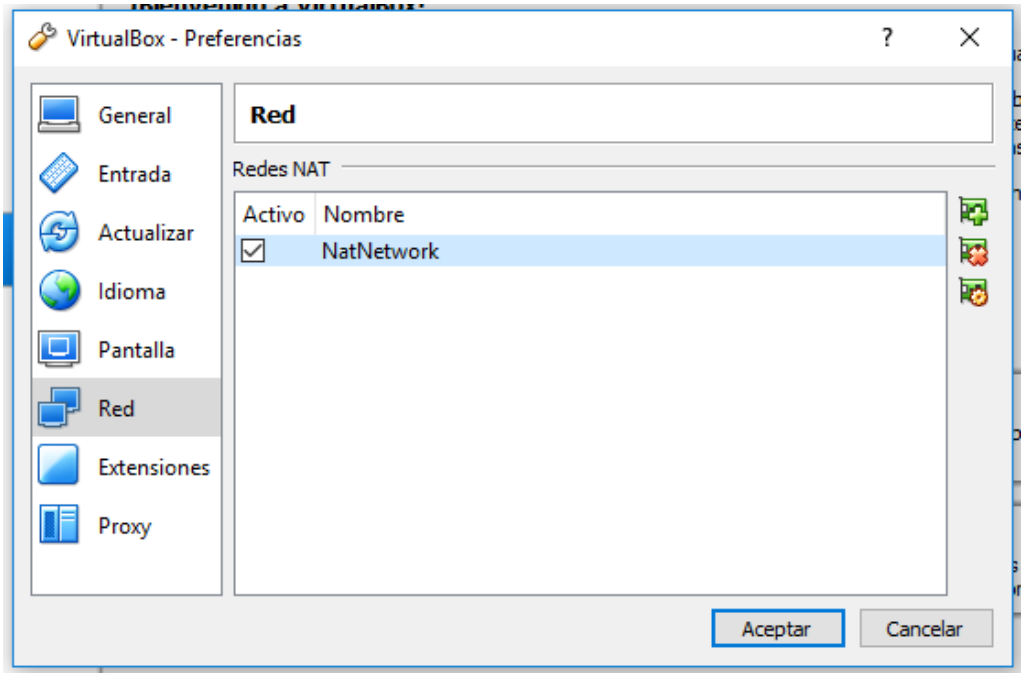
Figura 1. Creación de red NAT



Fuente: Autor

En la figura 1 se observa la ventana de preferencias y sobre esta la opción de red en la parte izquierda. Sobre la ventana desplegada se debe colocar el nombre de la red NAT que se desea crear, la red a utilizar, la máscara de subred y por último se da clic en el botón aceptar para guardar los cambios realizados.

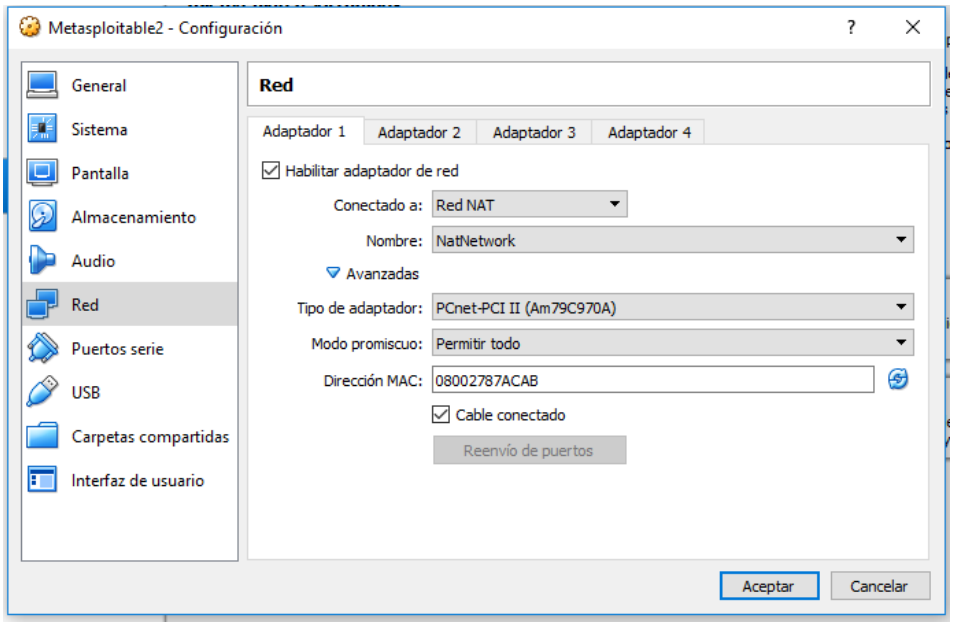
Figura 2. Ventana de configuración de red NAT.



Fuente: Autor

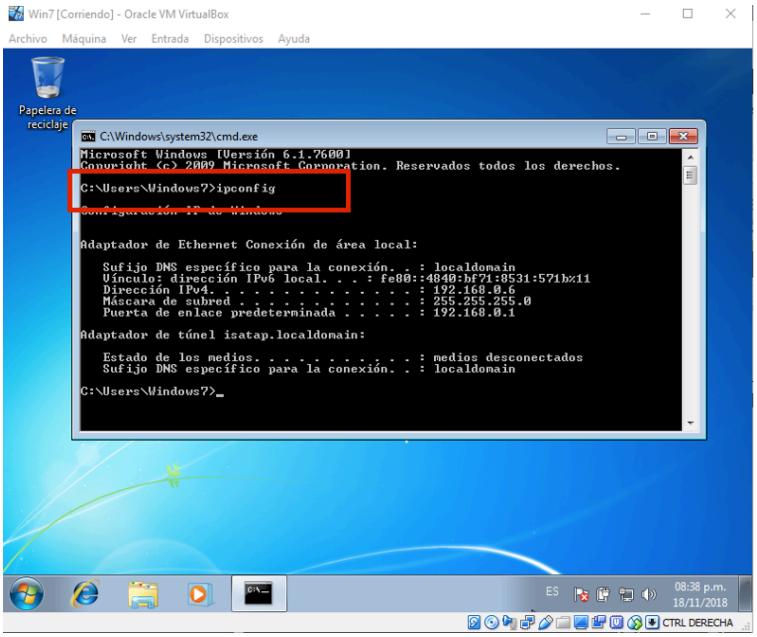
En la figura 2 sobre la opción de red se observa la red NAT creada, este paso se debe realizar en cada una de las máquinas virtuales a utilizar para que pueda existir comunicación entre ellas.

Figura 3. Configuración de red NAT en máquina virtual Linux *Metasploitable*



En la figura 3 se observa la configuración ya establecida sobre el adaptador de red y se identifica la red NAT sobre la cual se realizó la configuración.

Figura 4. Ventana CMD desplegando dirección IP máquina virtual con Windows 7

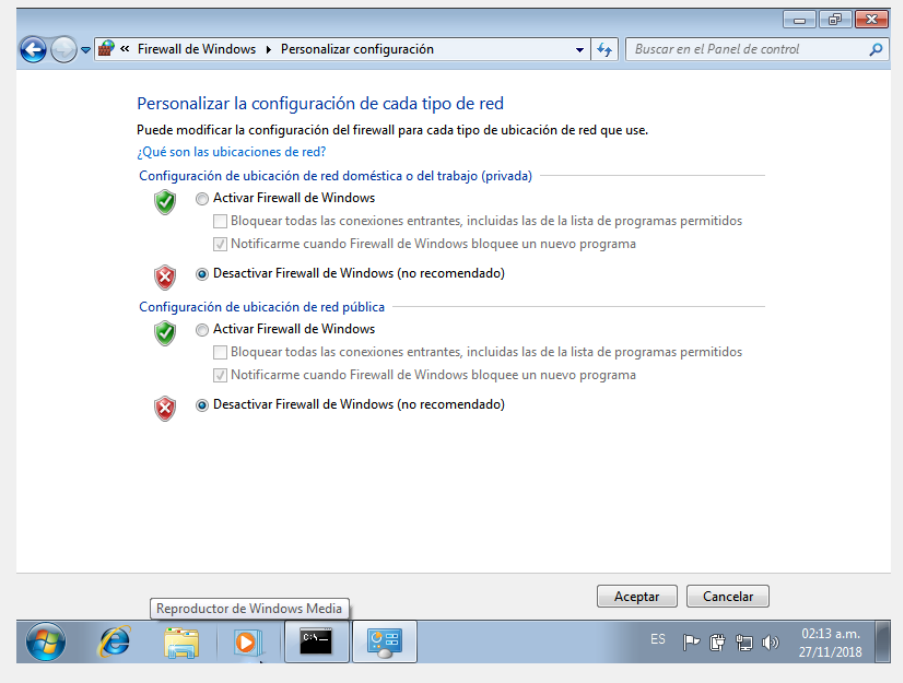


Fuente: Autor

En la figura 4 a través del comando ipconfig en la ventana de consola CMD se puede verificar la correcta configuración, esto debido a que la dirección ip asignada se encuentra dentro de la red creada previamente.

Otro paso importante para poder llevar a cabo el análisis de vulnerabilidad de manera correcta es desactivar el *firewall* en la máquina virtual con Windows 7, para ello desde el panel de control se debe ingresar a opciones y seguridad y allí buscar la opción *firewall*, posteriormente se debe seleccionar en cada una de las configuraciones ofrecidas, la opción de desactivación del *firewall* de *Windows* así como se observa en la figura 5.

Figura 5. Desactivación del firewall



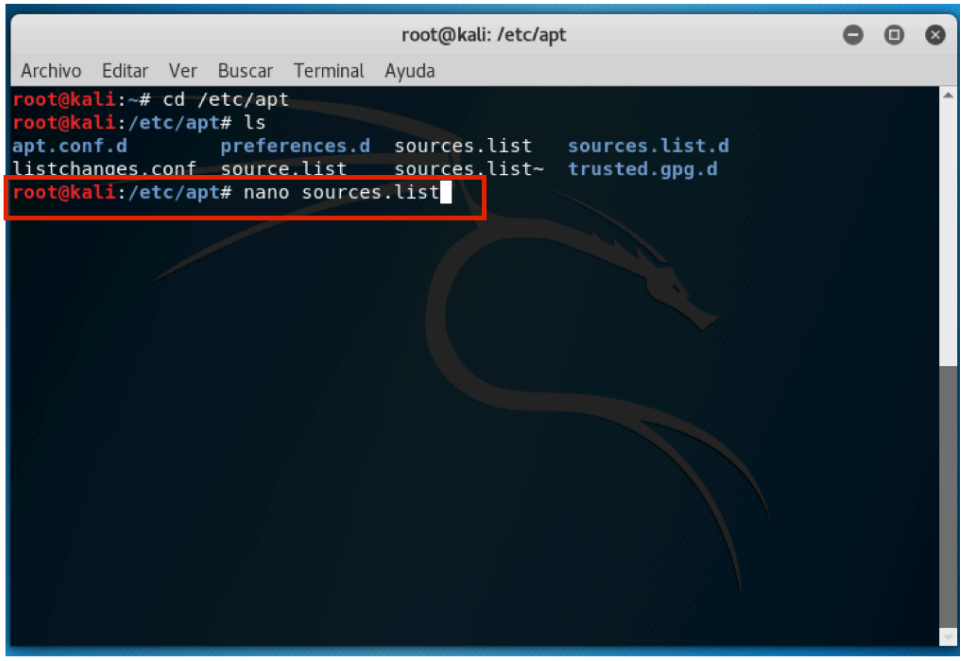
Fuente: Autor

7. PRUEBAS DE VULNERABILIDAD Y REALIZACIÓN DE ATAQUES

7.1 REALIZACIÓN DE ATAQUES

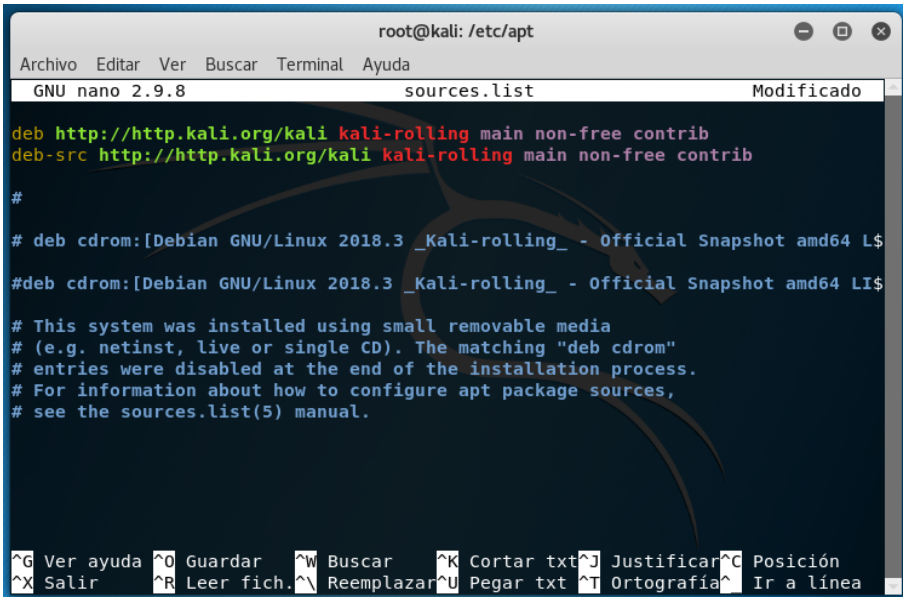
7.1.1 Ataque *Defacement*: A continuación, se presenta el paso a paso del proceso de actualización del sistema operativo Kali Linux. Lo primero a realizar es abrir una ventana terminal y ejecutar el comando nano sources.list, estando en la ubicación /etc/apt, esto es realizado para poder agregar las direcciones con los servidores desde los cuales se descargarán las actualizaciones, así como se observa en la figura 6.

Figura 6. Edición archivo sources.list



Fuente: Autor

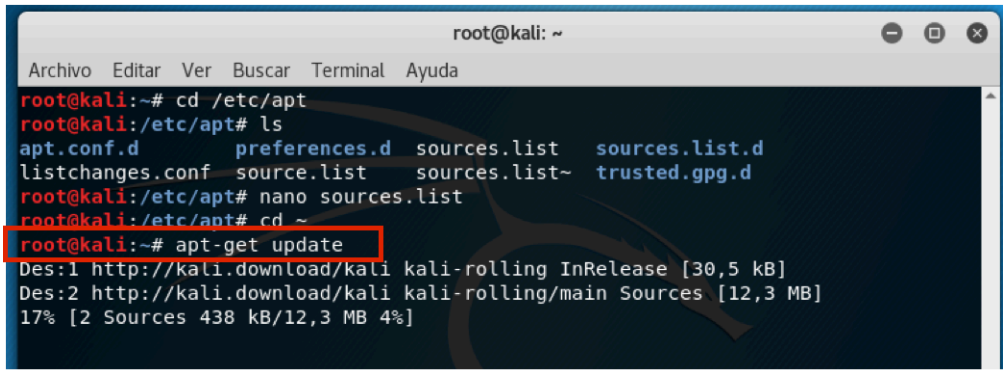
Figura 7. Adición de repositorios Kali



Fuente: Autor

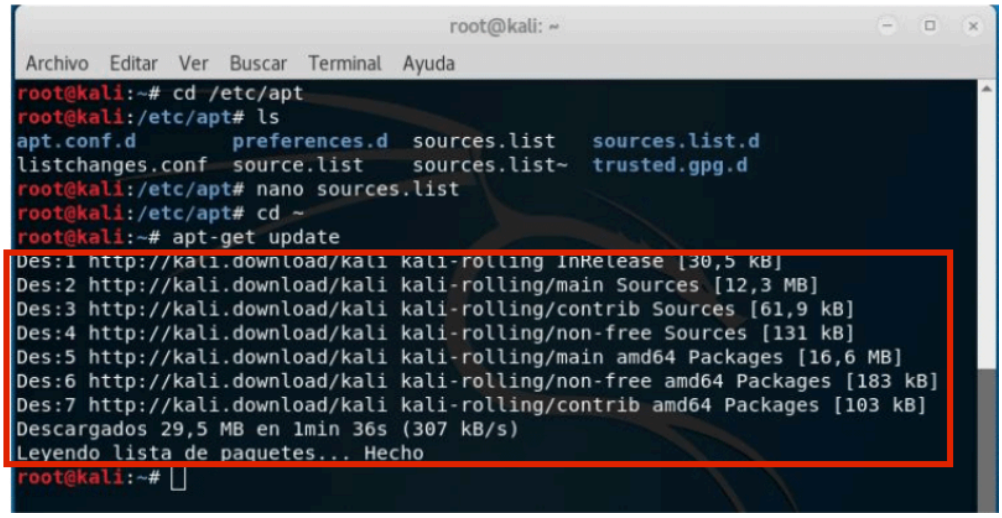
Una vez agregados los repositorios de Kali Linux se procede con la descarga de los paquetes de actualización a través de la ejecución del comando apt-get update.

Figura 8. Descarga de paquetes de actualización



Fuente: Autor

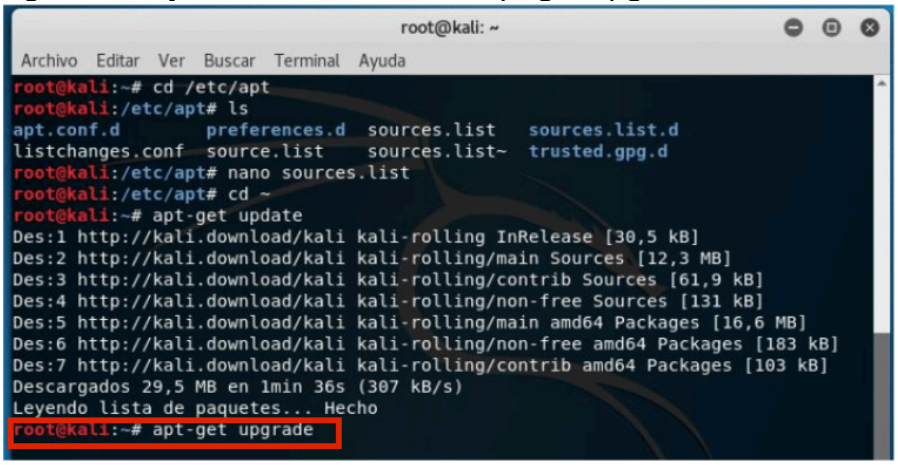
Figura 9. Finalización descarga de paquetes de actualización



Fuente: Autor

Seguidamente, se lleva a cabo la ejecución del proceso de instalación de los paquetes de actualización, esto a través del comando apt-get upgrade.

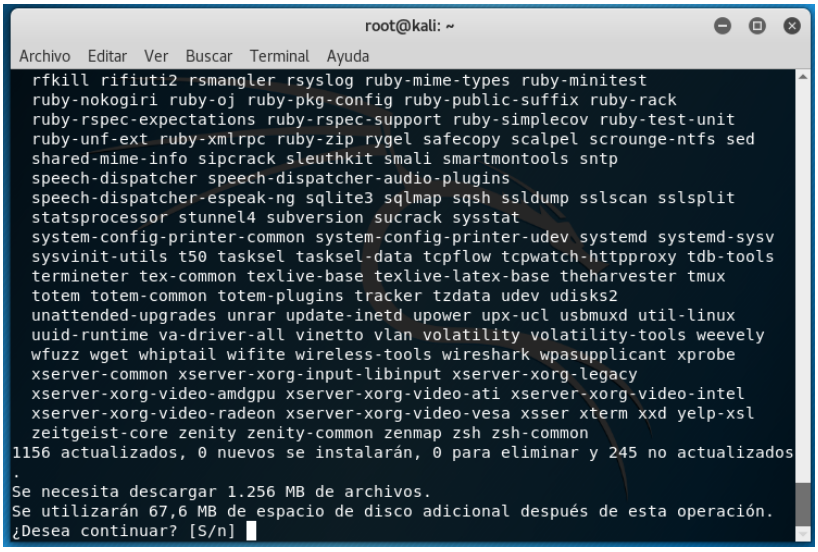
Figura 10. Ejecución de comando apt-get upgrade.



Fuente: Autor

En las imágenes siguientes se observa el proceso de instalación de los paquetes de actualización, este proceso se realizará de manera automática, sin embargo, en algunas ocasiones pedirá autorización para continuar con la actualización como se observa en la figura 11, a lo que se debe digitar S para continuar, esto debido a que las actualizaciones utilizarán espacio en el disco duro.

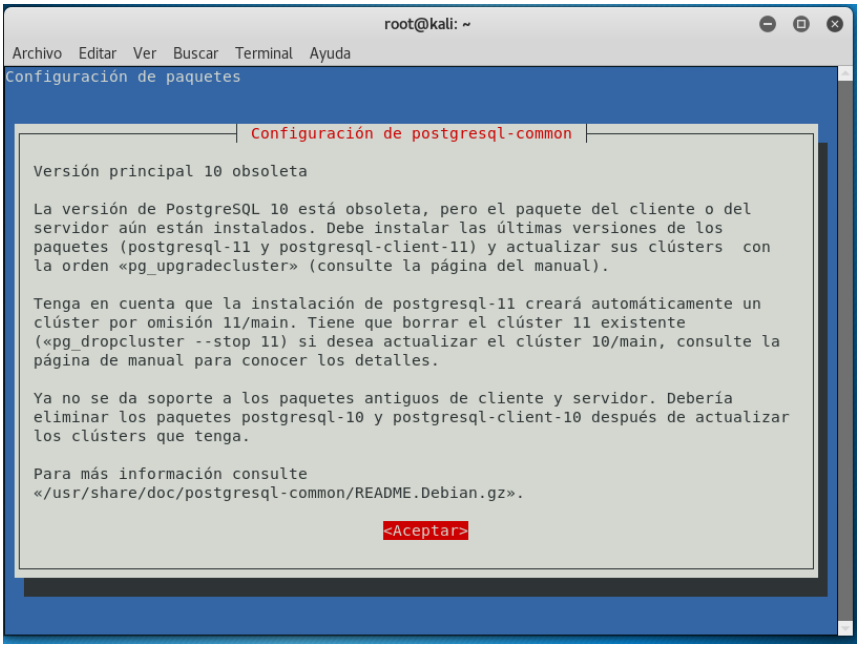
Figura 11. Progreso de actualización



Fuente: Autor

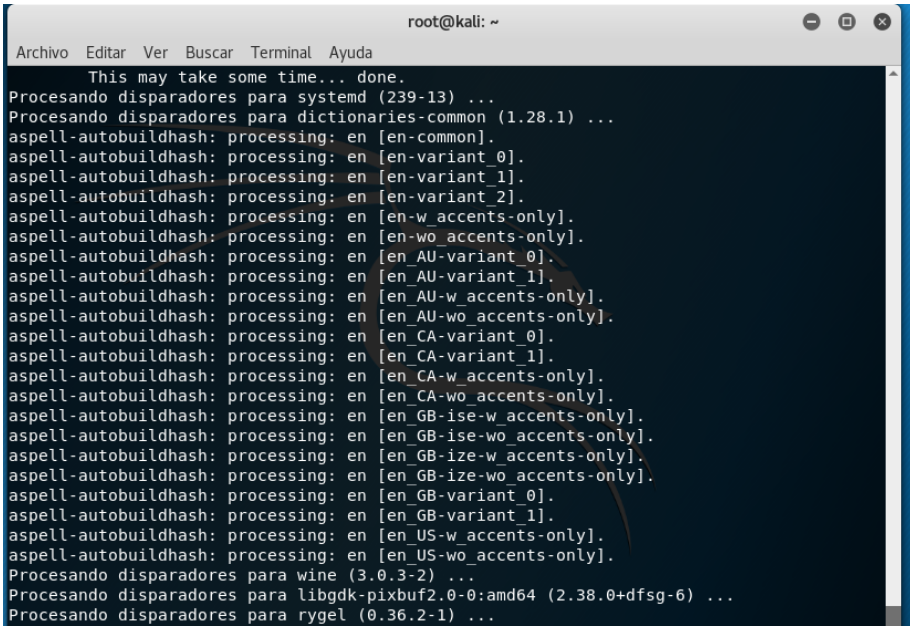
Durante el proceso de actualización se puede observar también la instalación de paquetes de postgresql. Cuando sea solicitado, se debe presionar la tecla *enter* con lo cual se estará aceptando la instalación y se continuará con el proceso.

Figura 12. Actualización de Postgresql



Fuente: Autor

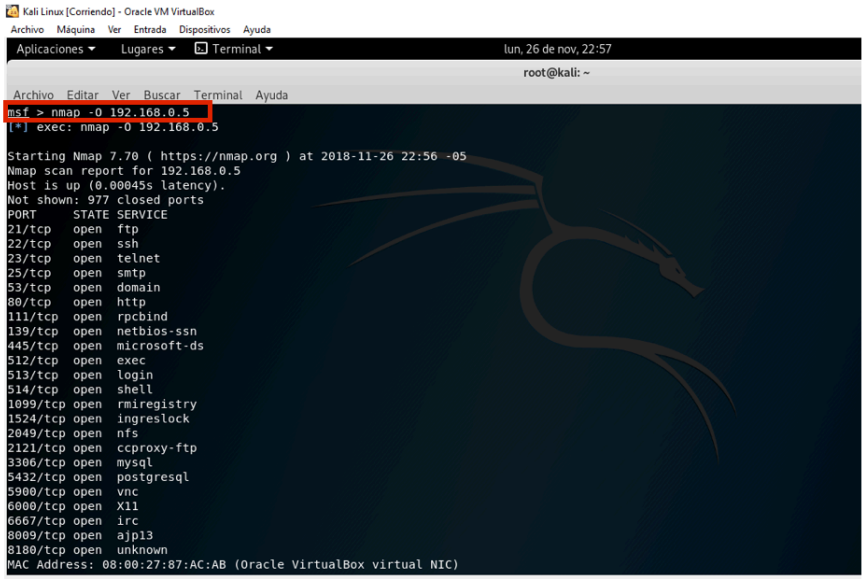
Figura 13. Finalización actualización de Kali Linux



Fuente: Autor

Una vez finalizado el proceso de actualización, se utilizará la herramienta NMAP la cual es utilizada para el escaneo de puertos, para ello desde la ventana terminal, se ingresa el comando nmap –o seguido de la dirección ip del equipo a escanear y posteriormente la tecla *enter* para su ejecución.

Figura 14. Escaneo de vulnerabilidades con NMAP

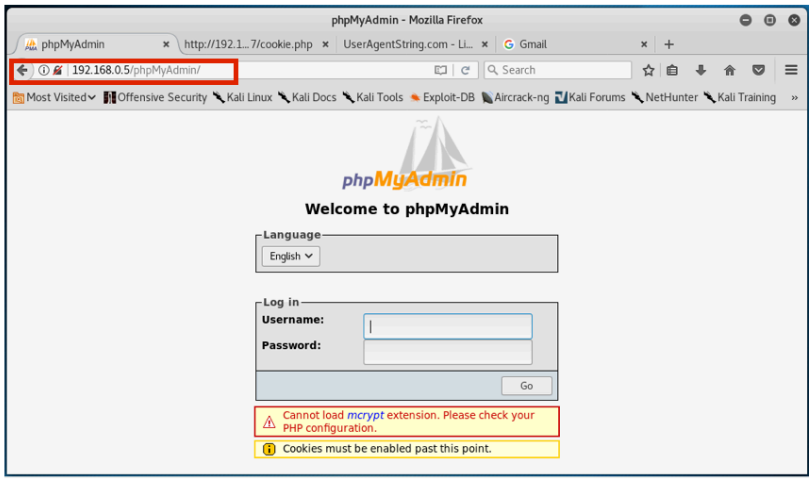


Fuente: Autor

El comando -o conjunto con el comando nmap permite identificar el sistema operativo alojado en la maquina atacada, a partir de ello, se pueden identificar posibles vulnerabilidades sobre este, con el fin de ser atacadas o realizar correcciones de seguridad.

Ejecución del ataque: El primer paso a realizar es la revisión de conexión con *PhpMyAdmin*, esto se realiza desde en el navegador, para ello se debe colocar la dirección ip del equipo en el navegador, así como se observa en la figura 15.

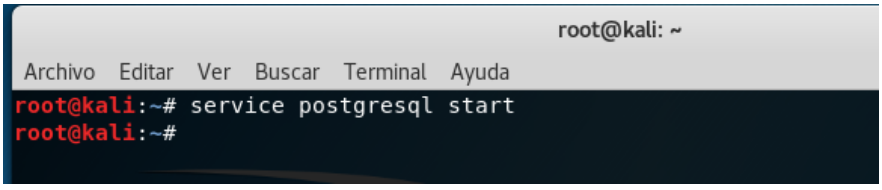
Figura 15. Revisión de conexión a phpMyAdmin de Linux *Metasploitable*



Fuente: Autor

Ahora desde la ventana terminal se procede a realizar la ejecución de postgresql mediante el comando *service* postgresql *start*

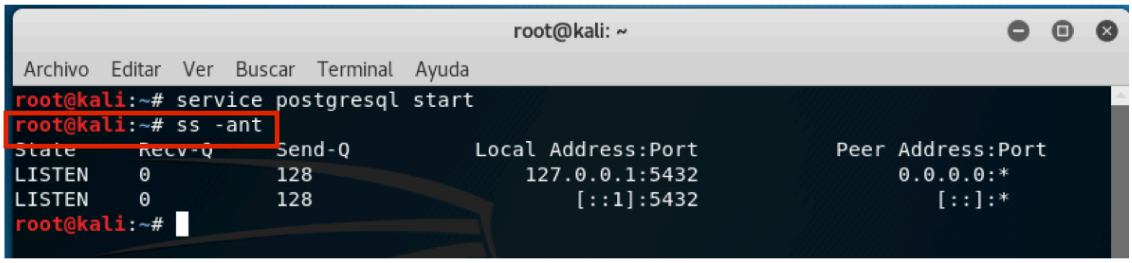
Figura 16. Ejecución de servicio *postgresql*



Fuente: Autor

Ventana terminal con la ejecución del comando ss -ant el cual permite la revisión de los puertos sobre los cuales se realiza la escucha.

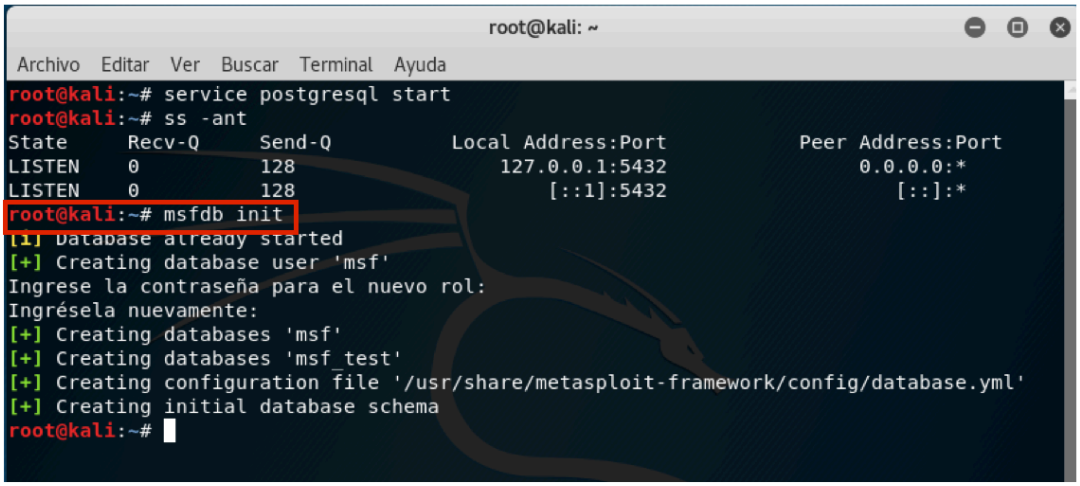
Figura 17. Revisión puertos de escucha



Fuente: Autor

En la figura 18 se observa la ventana terminal con la ejecución del comando msfdb init con el cual se inicializa la base de datos del *Metasploit*.

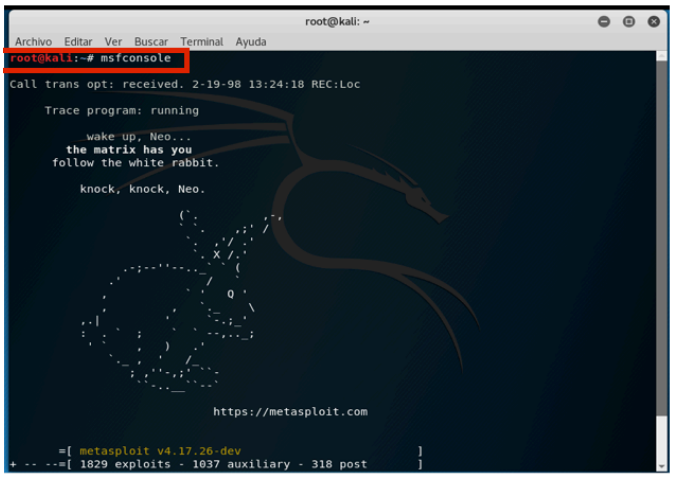
Figura 18. Inicio base de datos del *Metasploit Framework*



Fuente: Autor

Una vez se realiza el paso anterior, se debe ejecutar el *metasploite framework* a través del comando *msfconsole*, esto es realizado también desde la ventana terminal.

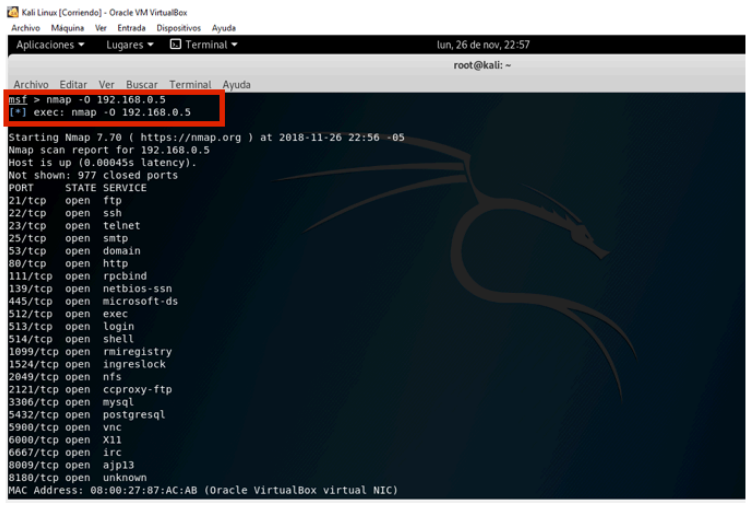
Figura 19. Ejecución del Metasploit Framework



Fuente: Autor

A continuación, se procede con la ejecución del comando nmap para verificar los puertos de escucha de la máquina virtual sobre la cual se encuentra instalado Linux Metasploitable.

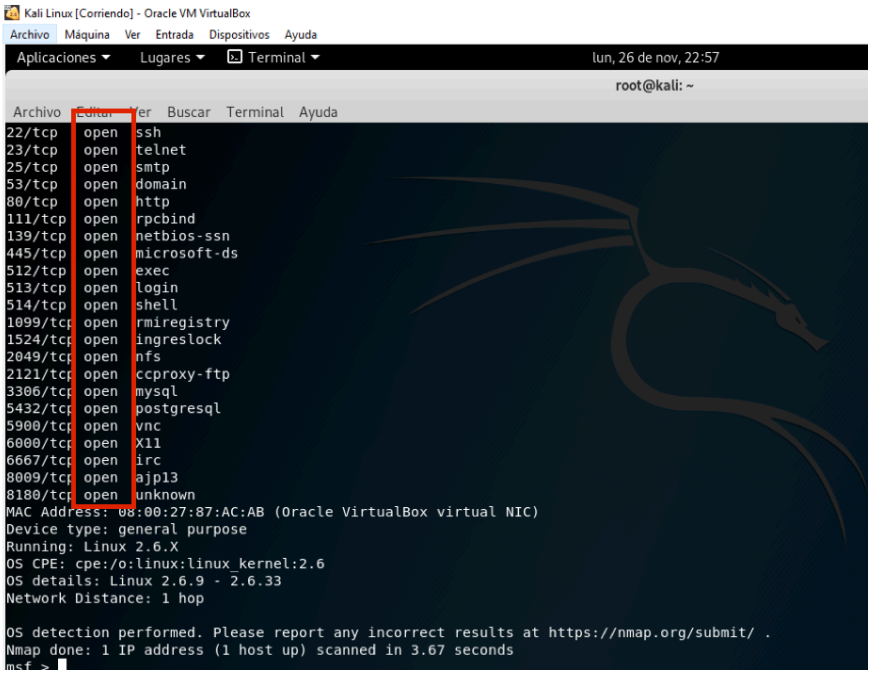
Figura 20. Escaneo de puertos con NMAP



Fuente: Autor

Al ejecutar el comando en la ventana terminal se observa el escaneo de puertos y el estado de cada uno de ellos ya sea abierto o cerrado como se puede apreciar en la figura 21.

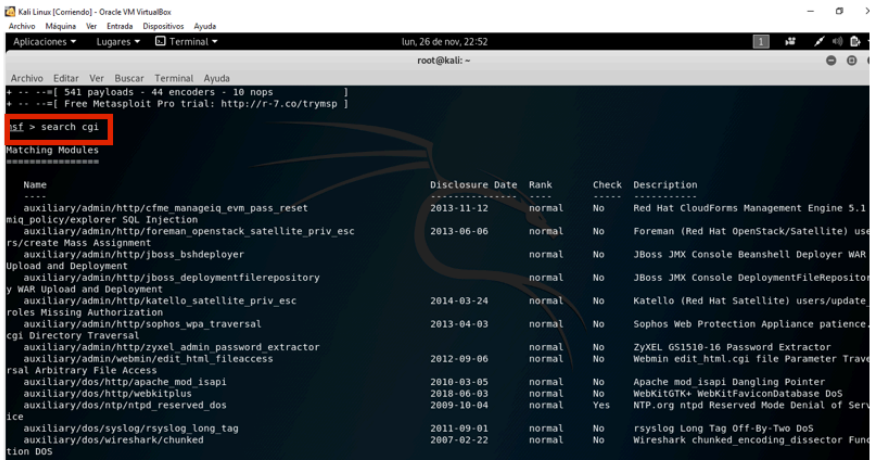
Figura 21. Estado de los puertos a través de NMAP



Fuente: Autor

Para poder iniciar la ejecución del ataque CGI a través de la URL del sitio, lo primero que se hará, será la búsqueda del *Exploit* a utilizar, para ello se escribe el comando *search cgi* con lo cual se listarán los ataques disponibles.

Figura 22. Búsqueda de exploit para vulnerabilidades cgi

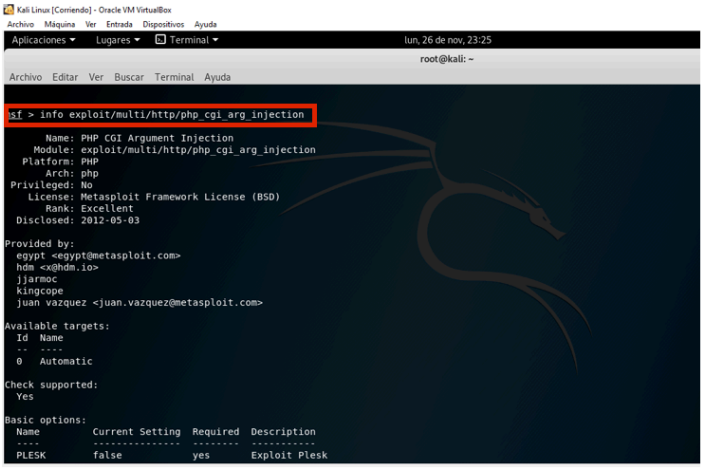


Fuente: El autor

Ahora se debe utilizar el comando *info* seguido del *Exploit* elegido (exploit/multi/http/php_cgi_arg_injection) como se observa en la figura 23. Con esto

se detalla la información del *exploit* con lo cual se verifica que sea el necesitado para la realización del ataque.

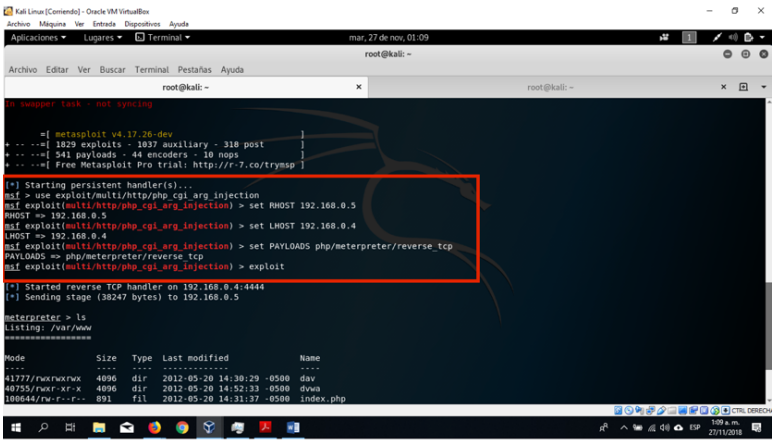
Figura 23. Detalle del *exploit* seleccionado



Fuente: Autor

Una vez corroborada la información se procede con la ejecución del *Exploi*t, para ello se utiliza el comando, *use* exploit/multi/http/php_cgi_arg_injection seguido de la Tecla *enter*

Figura 24. Uso del *exploit* seleccionado



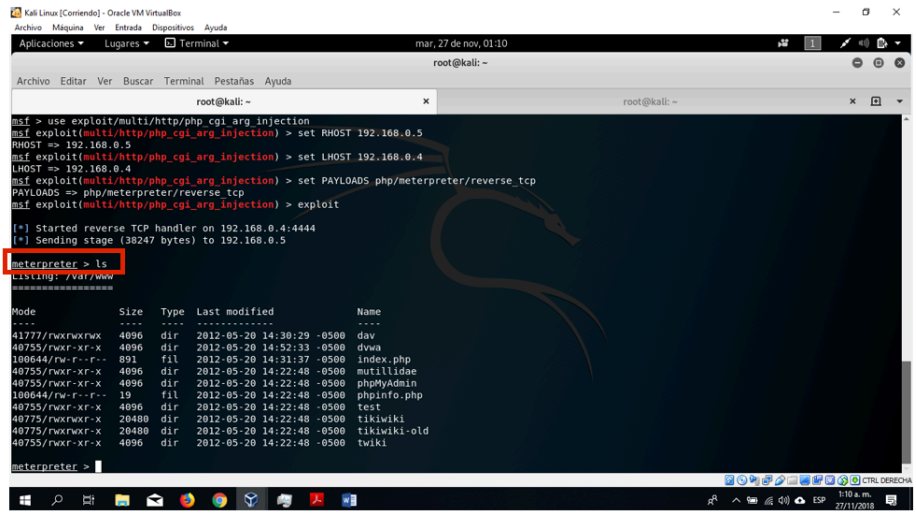
Fuente: Autor

Lo siguiente es proceder con la configuración del rhost y el lhost identificados como el equipo atacado y el atacante respectivamente, se utilizan los comandos set rhost 192.168.0.5 y set lhost 192.168.0.4, las direcciones ip utilizadas son las asignadas a cada máquina virtual de manera automática. Estas se pueden obtener mediante el comando ifconfig desde la ventana terminal.

Ahora se inyecta el payload con el comando set payloads php/meterpreter/reverse_tcp y se ejecuta a través del comando use *exploit*.

Una vez realizado, se debe obtener ingreso al sistema atacado, se pueden listar los archivos para verificar el ingreso, esto se realiza mediante la ejecución del comando ls como se observa en la figura 25.

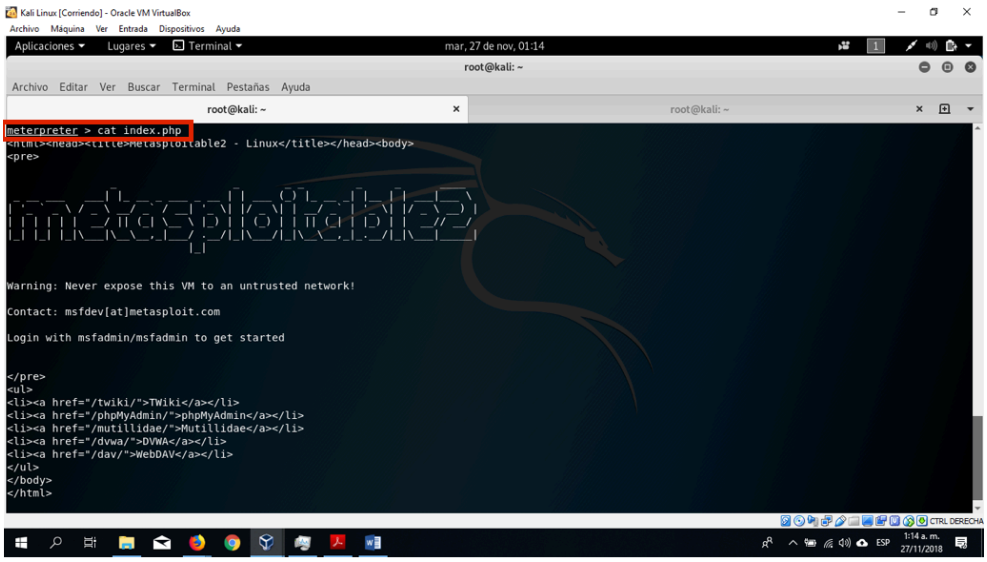
Figura 25. Ingreso desde Kali a máquina atacada



Fuente: Autor

Se procede con la búsqueda del archivo que contiene el index.php, una vez identificado a través del comando cat index.php se puede visualizar la información contenida en el archivo como se observa en la figura 26.

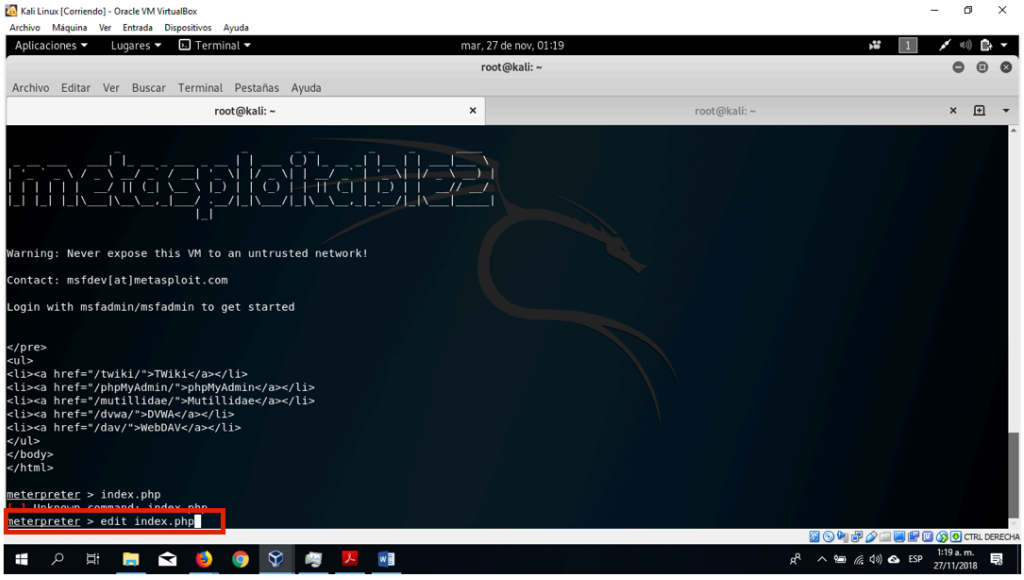
Figura 26. Apertura de archivo index.php



Fuente: Autor

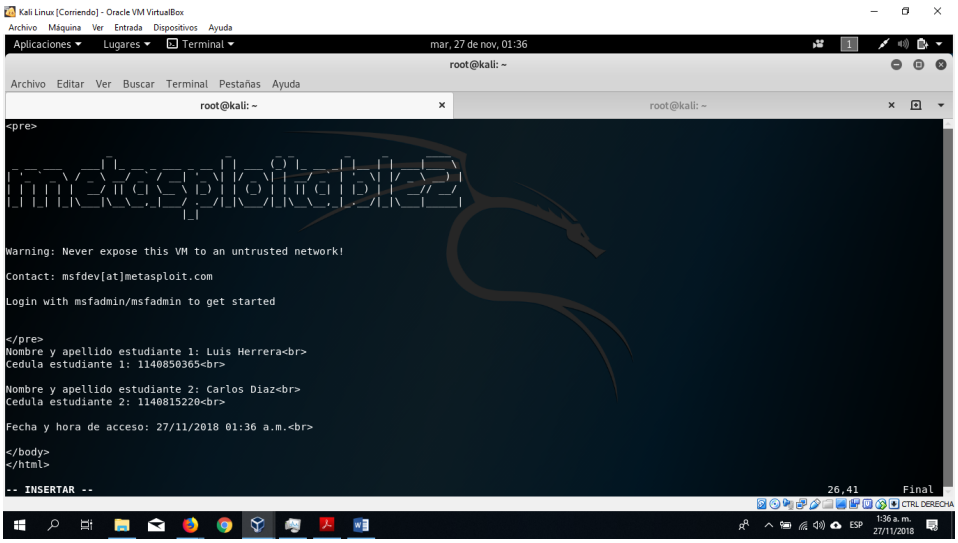
Para poder editar el archivo se ejecuta el comando edit, seguido del nombre del archivo, en este caso index.php

Figura 27. Uso del comando edit para edición del archivo



Fuente: Autor

Figura 28. Edición archivo index.php

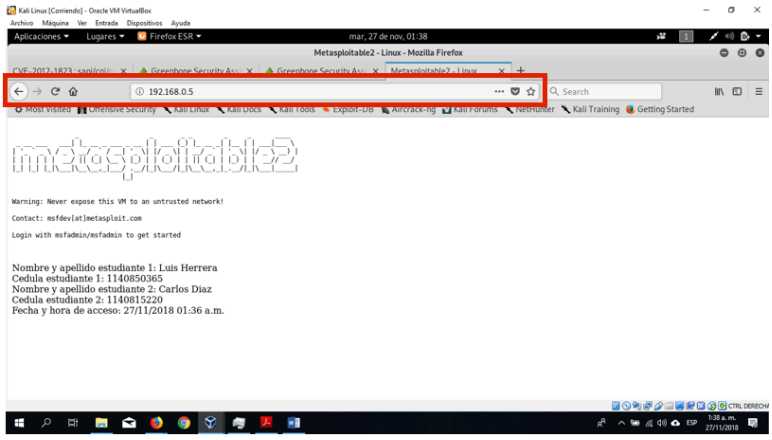


Fuente: Autor

Al finalizar la edición se presiona la tecla escape, luego la tecla shift y la tecla de dos puntos al mismo tiempo, luego la tecla w para guardar lo editado y la tecla q para salir del archivo.

Ahora se procede con la revisión del *índex* de la página atacada, esto se realiza abriendo el navegador y digitando la ip del servidor sobre el cual se alojó la página, en la figura 29 se puede evidenciar que el ataque de *Defacement* se realizó de manera correcta.

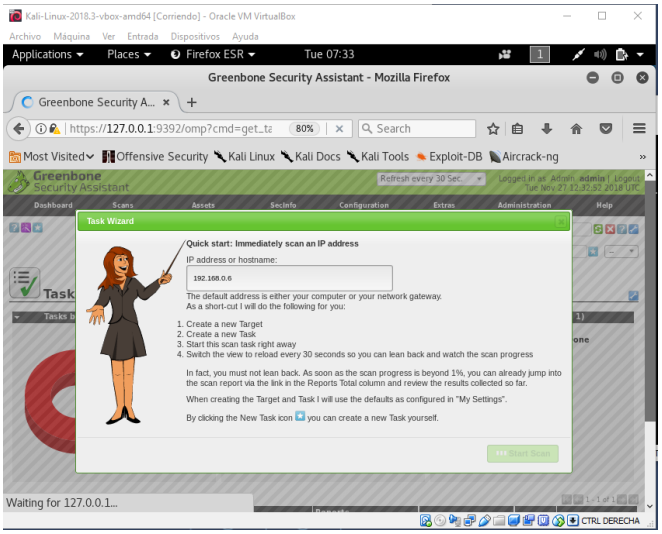
Figura 29. Ataque Defacement realizado



Fuente: Autor

7.1.2 Ataque *Eternal Blue*: Desde Kali Linux se procede a ejecutar la aplicación Openvas la cual es utilizada para el análisis de vulnerabilidades. Esto se realiza desde un navegador web digitando la dirección IP y el puerto sobre el cual se realizó la configuración. Se desplegará una ventana emergente sobre la cual se digitará la IP del equipo al cual se le realizará el escaneo y posteriormente de da clic sobre el botón *start scan*.

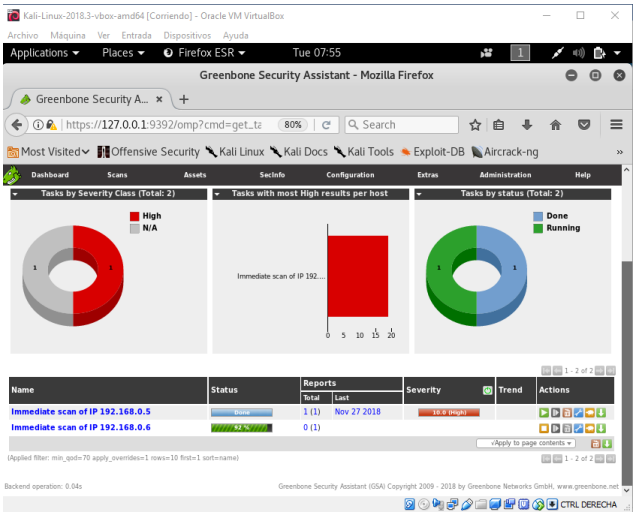
Figura 30. Inicio de escaneo con OpenVas



Fuente: Autor

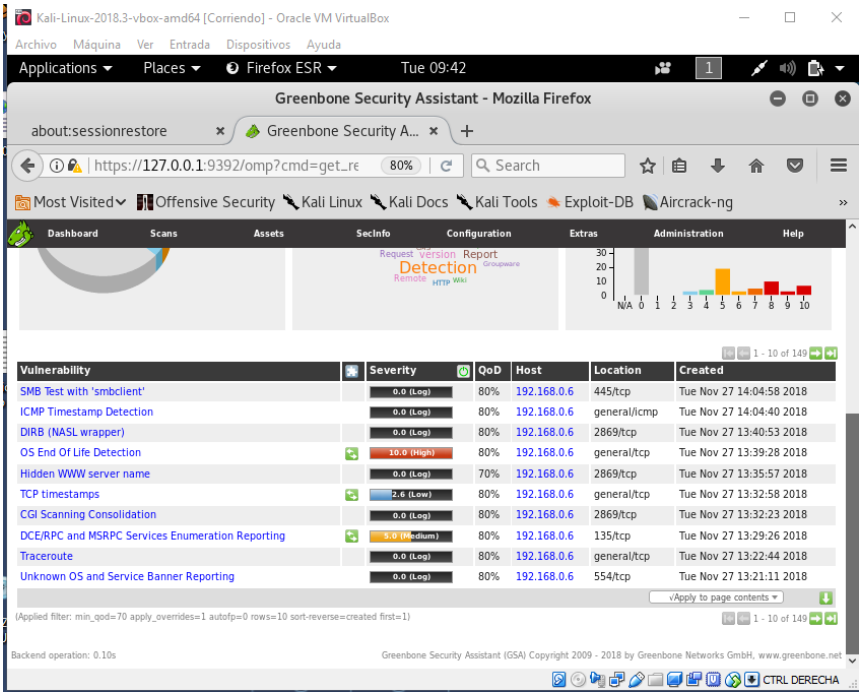
En la Figura 31 se observa el resultado de los análisis ejecutados hacia la máquina virtual con Windows 7.

Figura 31. Gráficas de resultado de análisis



Fuente: Autor

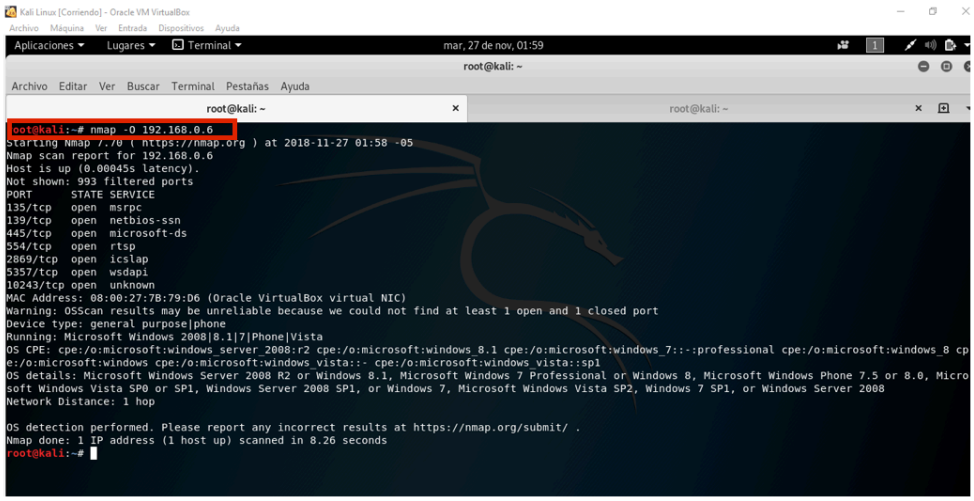
Figura 32. resultado de vulnerabilidades encontradas



Fuente: Autor

Una vez finalizado el proceso de escaneo de vulnerabilidades con OpenVas se procede con el escaneo de puertos ejecutando desde el terminal el comando nmap -o hacia la máquina con Windows 7 como se observa en la figura 33.

Figura 33. Escaneo de vulnerabilidades con Nmap



Fuente: Autor

A través del escaneo realizado se pudieron evidenciar varias fallas de seguridad que comprometen la integridad del equipo, una de ellas es el estado del sistema operativo, del cual se advierte que su ciclo de vida ha terminado. Cuando esto sucede las marcas terminan el soporte y no brindan más correcciones a fallas, por lo que las fallas de seguridad presentadas no pueden ser corregidas mediante actualizaciones.

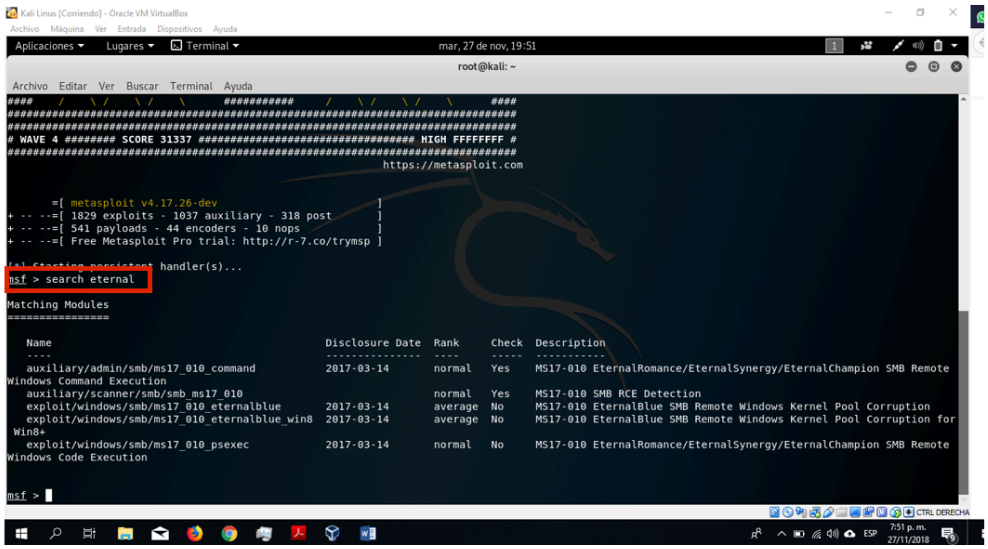
Si se observa el escaneo realizado con nmap en la figura 33 también se evidencian fallos en la seguridad, ya que se encuentran puertos abiertos por los cuales se pueden ejecutar ataques, en ejemplo de estos es el ataque conocido como *Eternal Blue* el cual se ejecuta a través del puerto 445.

Ejecución de los ataques

Keylogger

Para la realización de este ataque lo primero a realizar es la ejecución de los comandos postgresql start, ss-ant y msfdb init desde una ventana terminal. Posteriormente se ingresa el comando msfconsole para iniciar el *Metasploit Framework*. Luego se ingresa el comando search cgi para buscar un *exploit* que permita explotar el fallo.

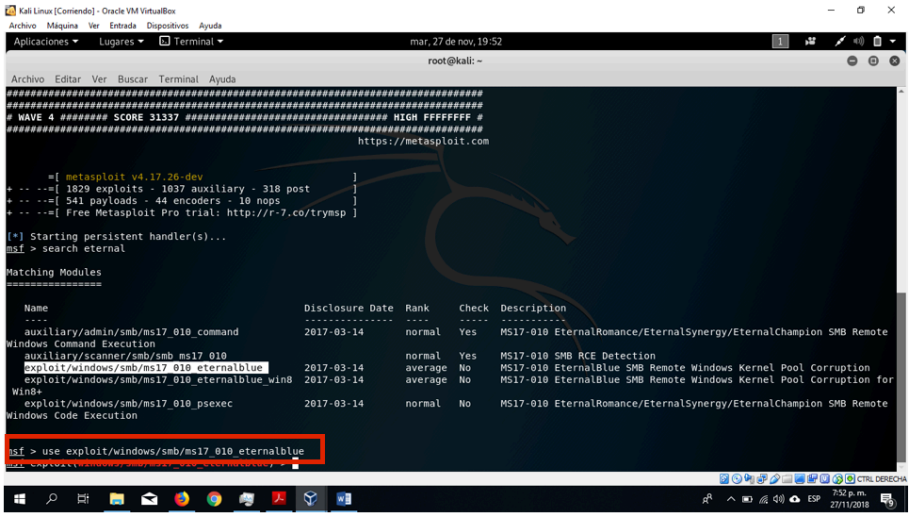
Figura 34. Ejecución del Metasploit Framework



Autor: Fuente

Una vez se ingresa al metasploit se debe buscar el *exploit* a utilizar, para ello se utiliza el comando *search eternal*. Figura 34

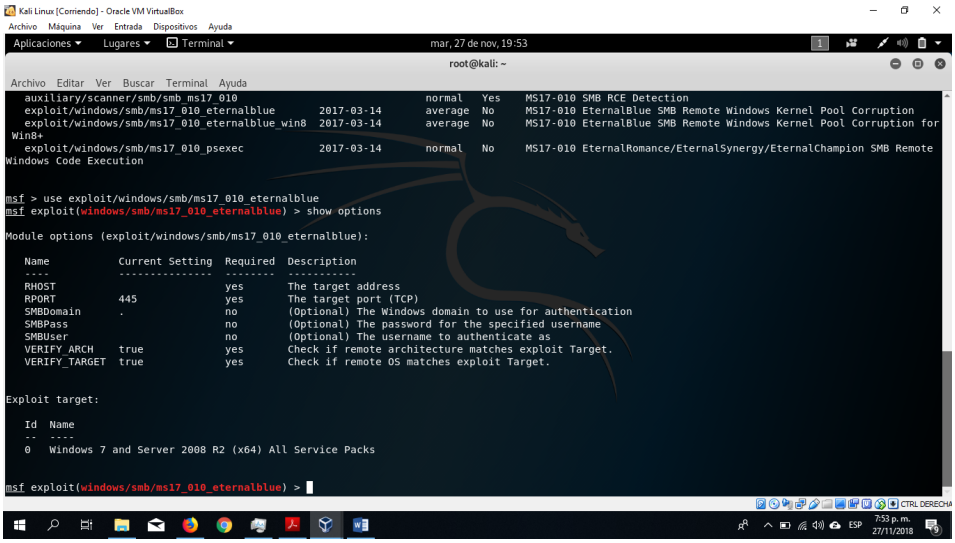
Figura 35. Selección exploit



Fuente: Autor

Una vez localizado el exploit a utilizar, se debe iniciar usando el comando use, seguido de la ruta del *exploit*.

Figura 36. Configuración del *exploit*

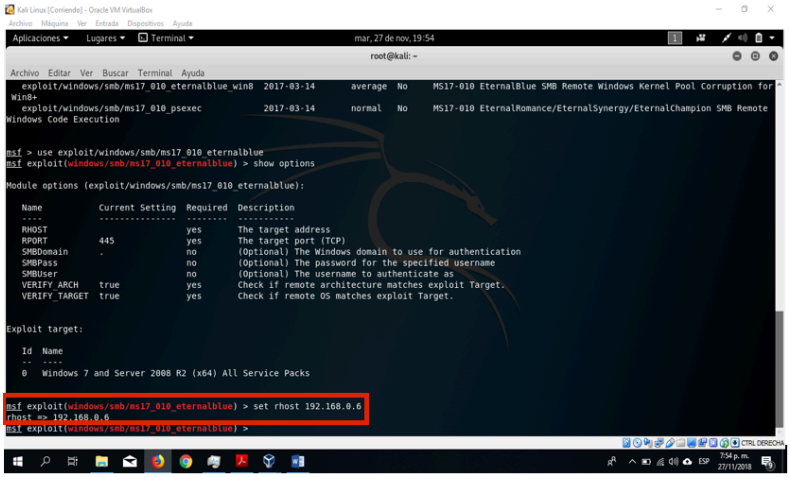


Fuente: Autor

Ahora se deben definir las direcciones ip del equipo atacado y del equipo atacante, para ello se utilizan los comandos rhost y lhost seguidos de la ip de cada uno de los equipos, de igual manera se realizará la inyección del payload.

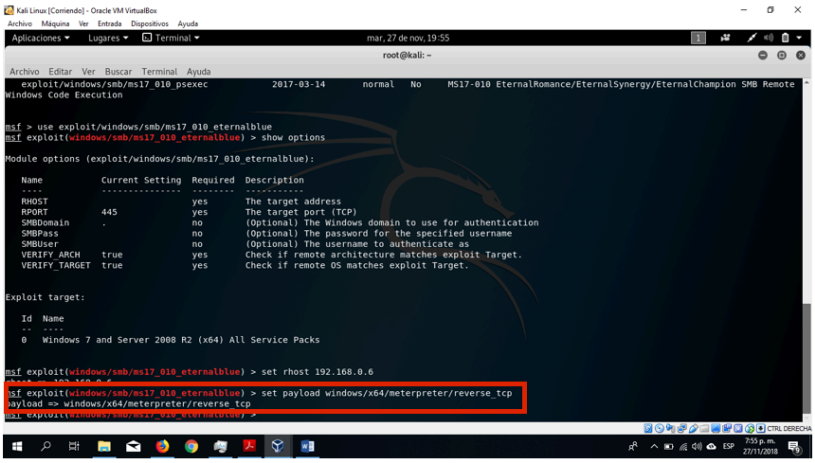
En las figuras 37,38,39 y 40 se aprecia la configuración del equipo sobre el cual se ejecutará el ataque y el paso a paso de los comandos ejecutados.

Figura 37. Configuración del exploit



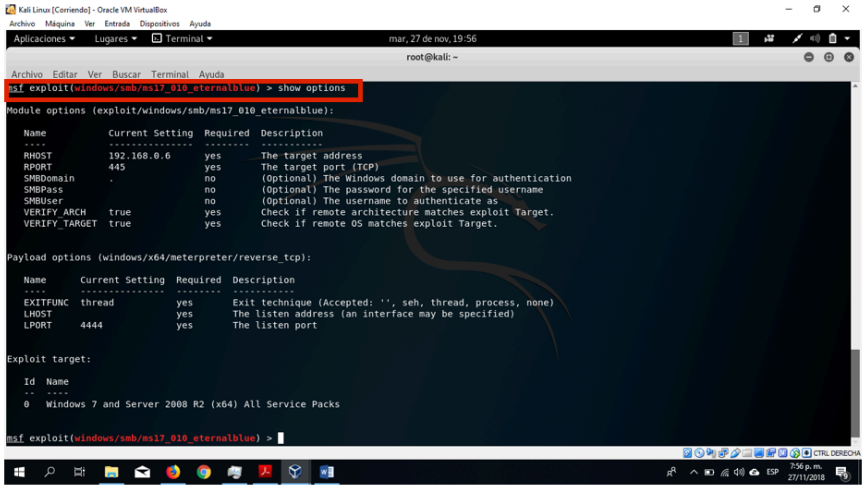
Fuente: Autor

Figura 38. Configuración del exploit



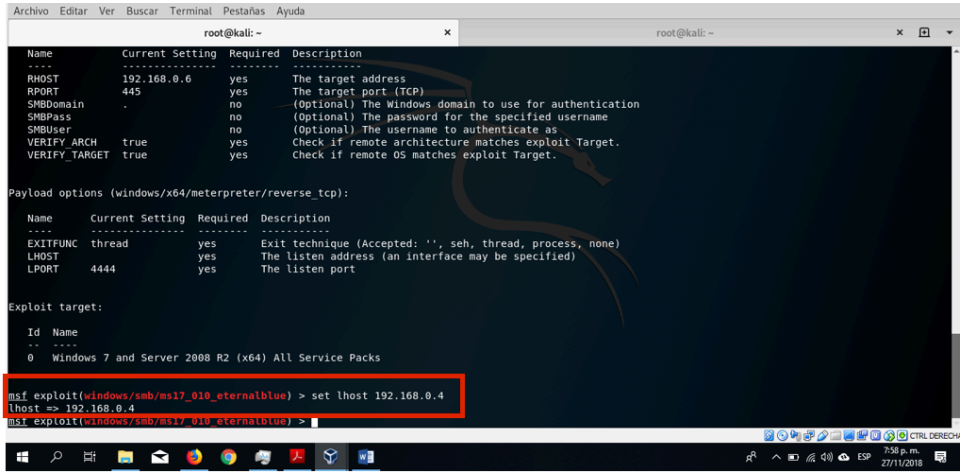
Fuente: Autor

Figura 39. Configuración del exploit



Fuente: Autor

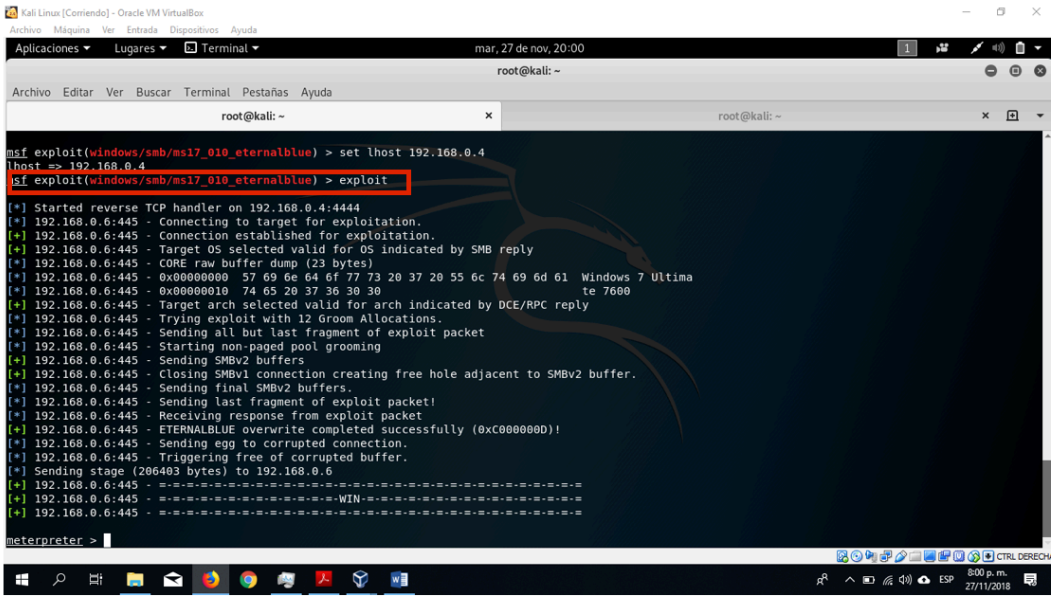
Figura 40. Configuración del exploit



Fuente: Autor

Una vez realizada la configuración de los equipos a través del comando set tanto para el lhost como para el rhost, se lanza el exploit utilizando el comando *exploit* como se observa en figura 41.

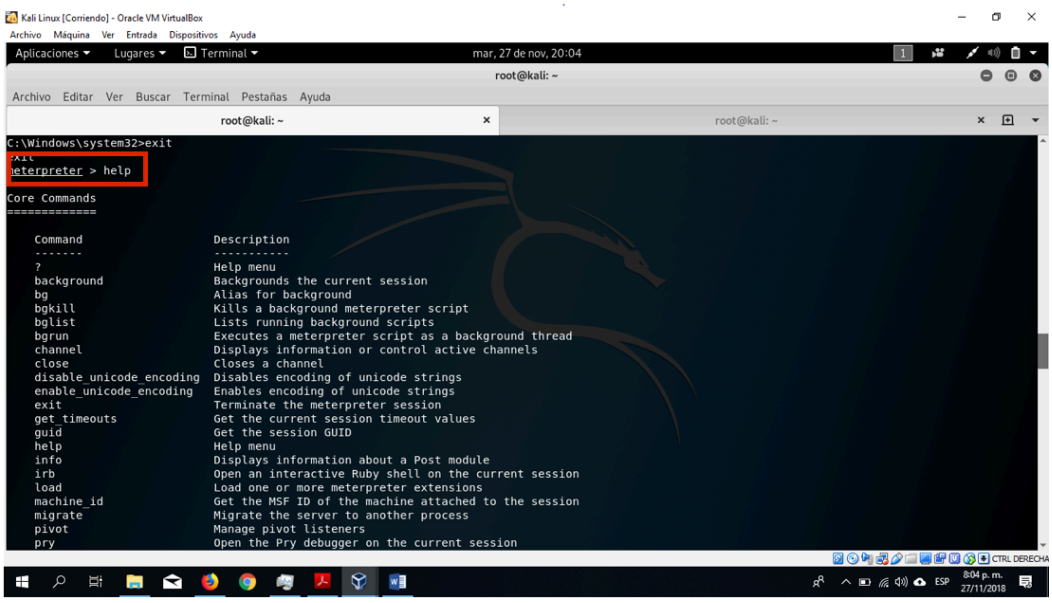
Figura 41. Ejecución exploit



Fuente: Autor

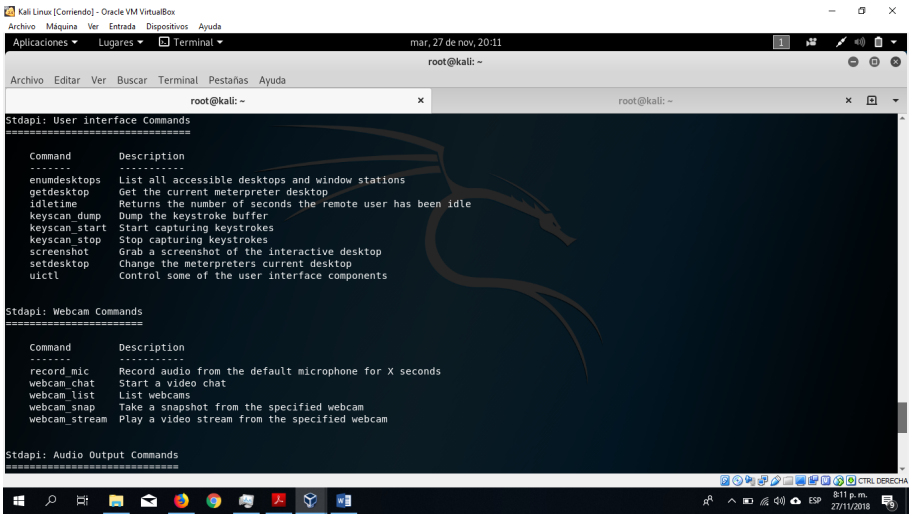
Una vez lanzado el *exploit* y se esté por fuera del *meterpreter*, se utiliza el comando *help* donde se listarán todas las opciones disponibles como se observa en la figura 42.

Figura 42. Listado de comandos



Fuente: Autor

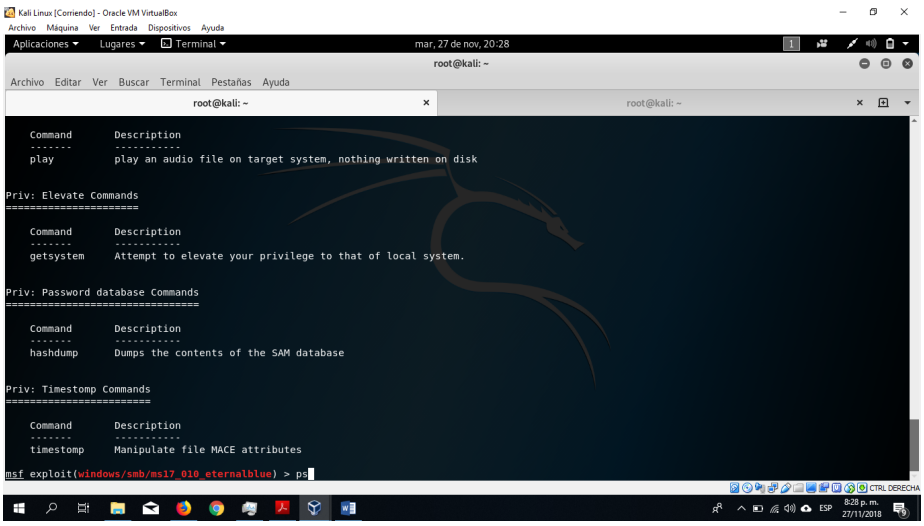
Figura 43. Listado de comandos del exploit



Fuente: Autor

En la figura 43 se observa la continuación del listado de comandos del *exploit*.

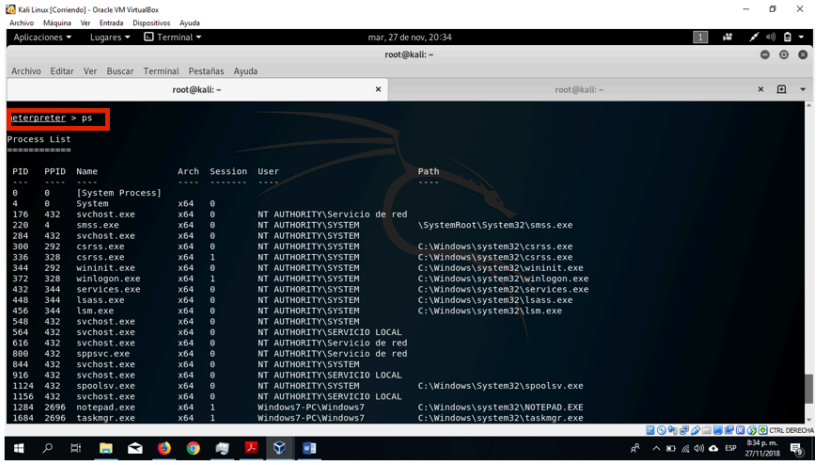
Figura 44. Listado de comandos



Fuente: Autor

Para que el ataque pueda ser ejecutado se debe utilizar un proceso activo en el equipo remoto, para ello se realiza un escaneo de los procesos activos ejecutando el comando ps, en este caso se utilizará el proceso del bloc de notas.

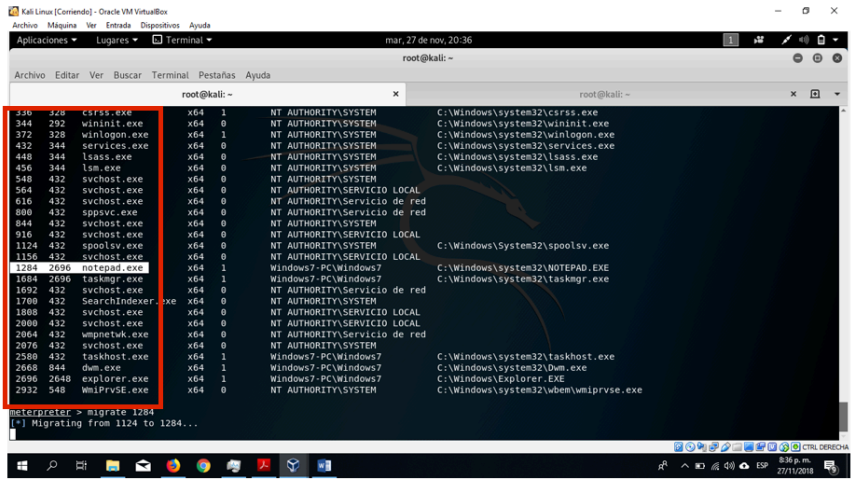
Figura 45. Revisión de procesos activos en Windows 7



Fuente: Autor

En la figura 45 se observa el listado de procesos activos en el equipo a ser atacado.

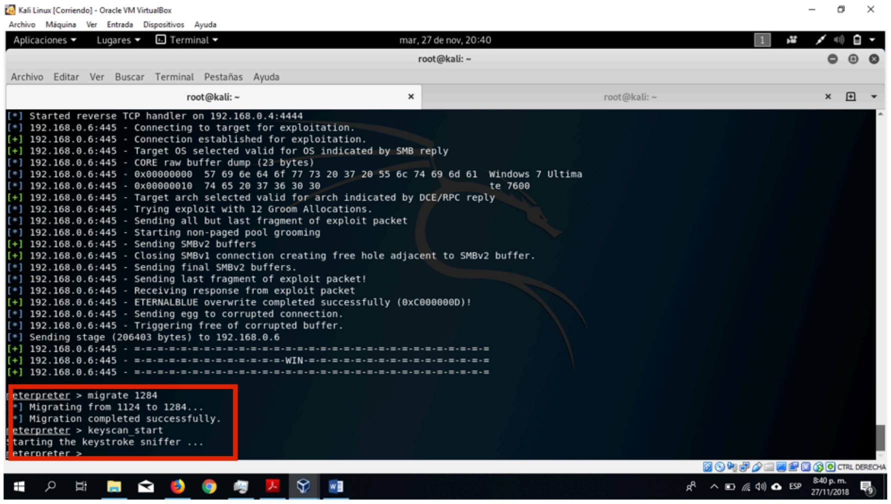
Figura 46. Listado de procesos activos



Fuente : Autor

Una vez se ha localizado el proceso, se debe digitar el código de identificación de este, antecedido del comando *migrate* como se observa en la figura 46, posteriormente se lanza el ataque de captura a través del comando keyscan_start.

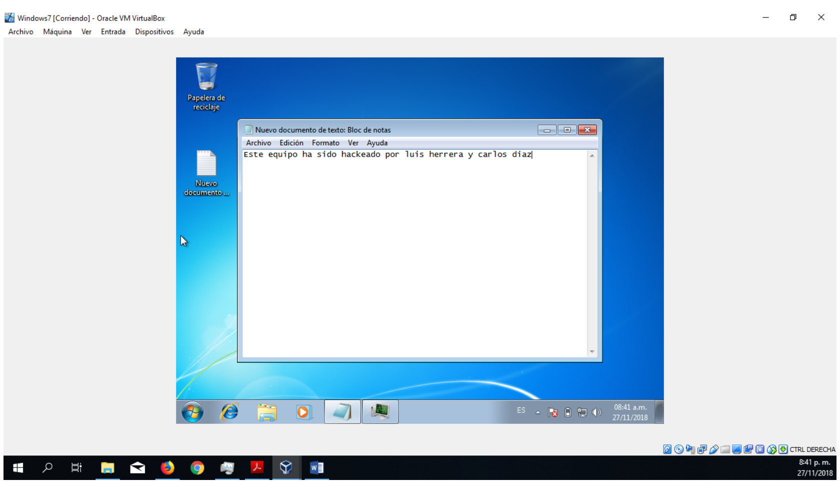
Figura 47. Ejecución keylogger



Fuente: Autor

Una vez en el equipo atacado se realice la ejecución del programa bloc de notas, cualquier tipo de información digitada sobre este, será capturada por el atacante.

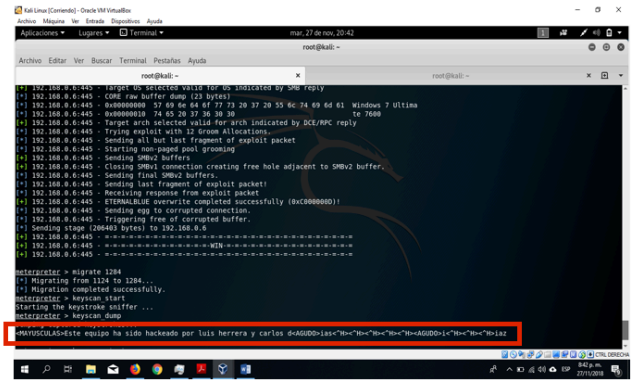
Figura 48. Ingreso de texto en bloc de notas



Fuente: Autor

En la máquina con Kali Linux se puede observar la captura de la información digitada, resultando así un ataque exitoso.

Figura 49. Visualización texto capturado

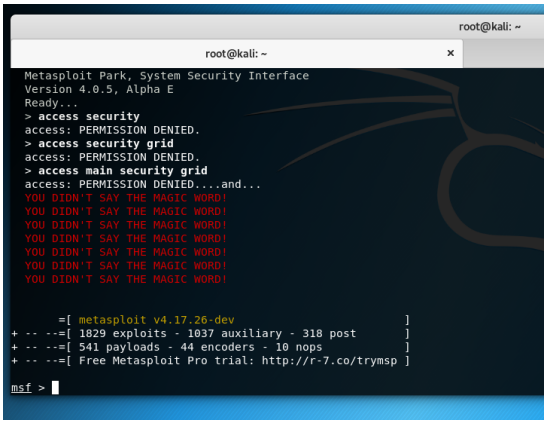


Fuente: Autor

Cámara Web

A continuación, se describe el paso a paso del proceso de activación de la cámara web de un equipo remoto. El primer paso para ello es el ingreso al *metasploit*.

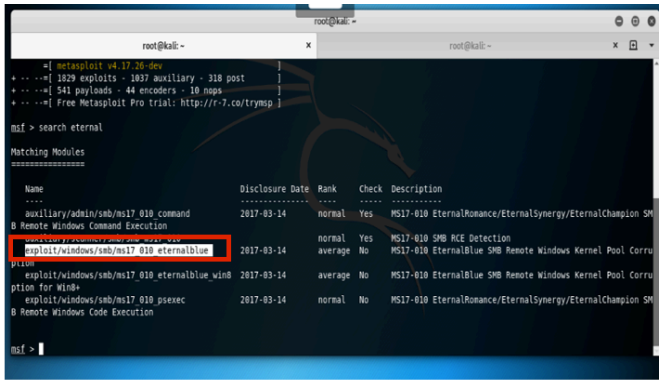
Figura 50. Inicio de metasploit



Fuente: Autor

Para ello se utiliza el *exploit* que ataca la vulnerabilidad hallada en *Eternalblue* de Windows.

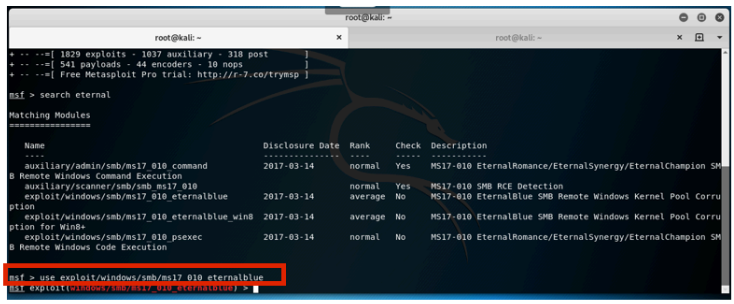
Figura 51. Selección del exploit



Fuente: Autor

Sobre la ventana terminal se escribe el comando *search eternal* y se presiona la tecla *enter* para su ejecución. Una vez listados los ataques disponibles, se selecciona el relacionado con la vulnerabilidad *eternal blue*, para lo cual se procede a copiar la ruta como se observa en la figura 51, luego mediante el comando *use*, seguido de la ruta copiada y la tecla *enter* se ingresa a la configuración del *exploit*.

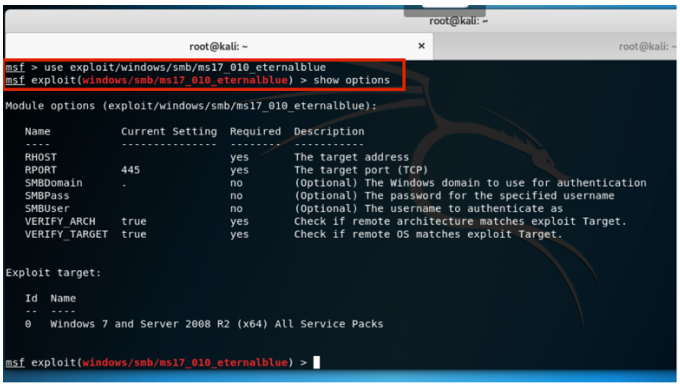
Figura 52. Selección del *exploit*



Fuente: Autor

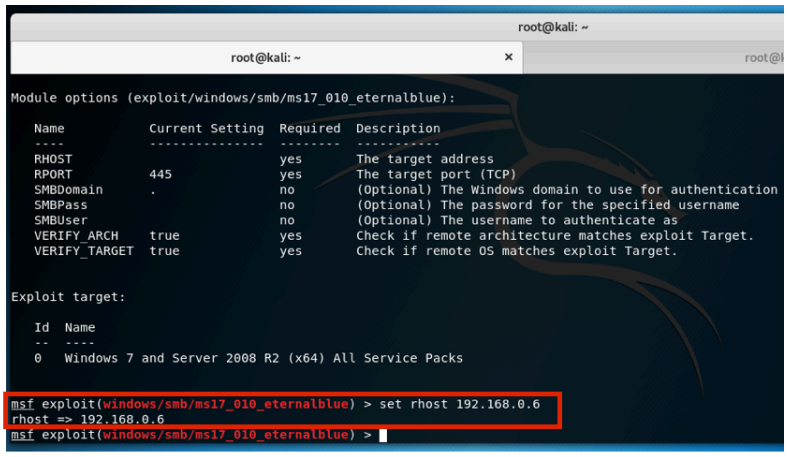
Se debe realizar la configuración de la ip del equipo local y del equipo destino a través de los comandos lhost y rhost respectivamente, para luego realizar la inyección del *payload* a través del comando *set payload*. Figura 54

Figura 53. Configuración del *exploit*



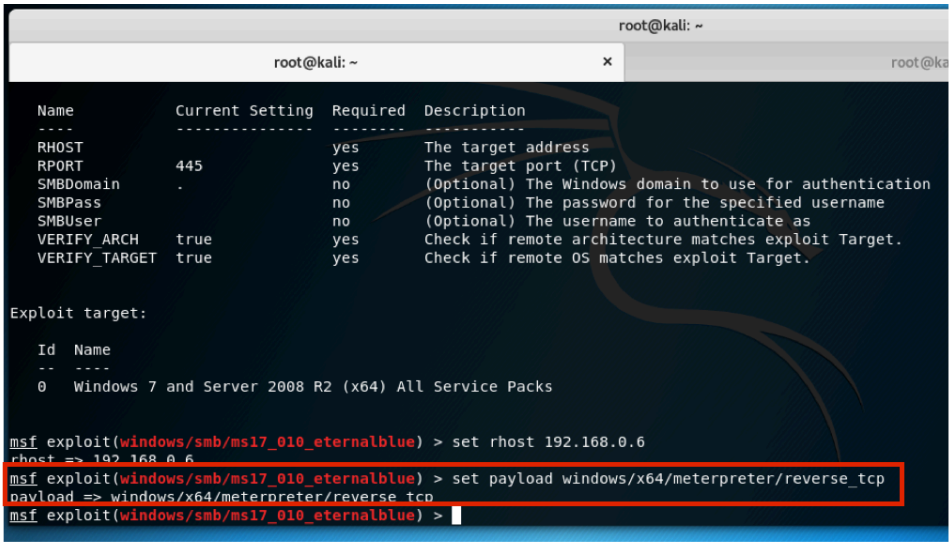
Fuente: Autor

Figura 54. Configuración del *exploit*



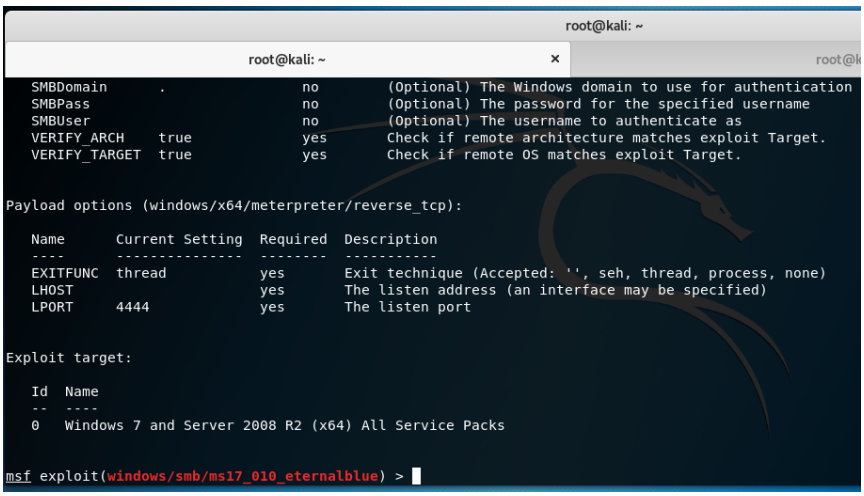
Fuente: Autor

Figura 55. Configuración del *exploit*



Fuente: Autor

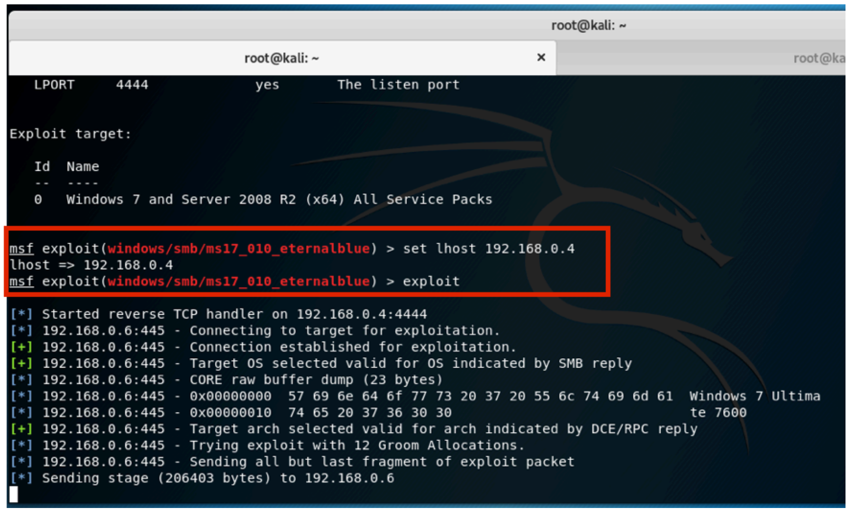
Figura 56. Configuración del *exploit*



Fuente: Autor

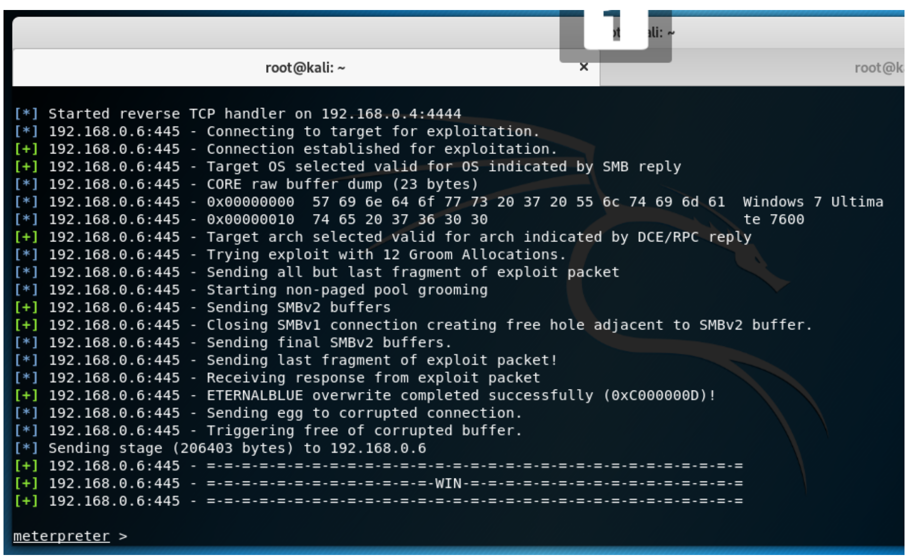
Una vez terminada esta configuración se procede a lanzar el *exploit*, desde *meterpreter,* ejecutando el comando *exploit* desde la ventana terminal.

Figura 57. Ejecución del *exploit*



Fuente: Autor

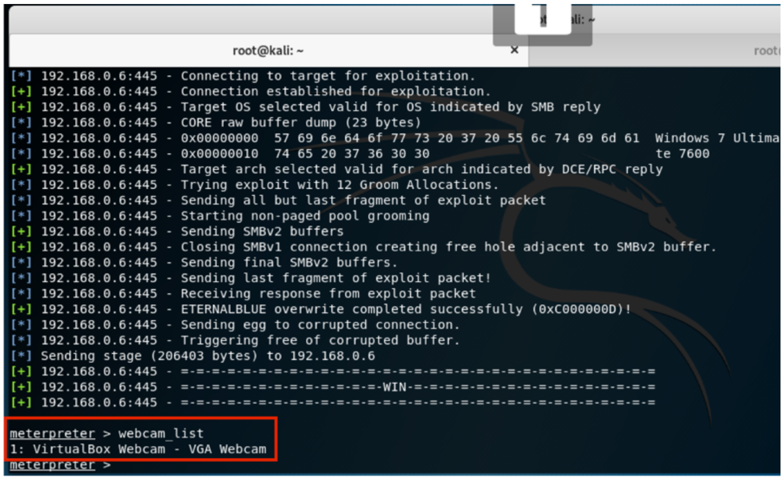
Figura 58. Ejecución del *exploit*



Fuente: Autor

Una vez obtenido el acceso al equipo atacado, utilizando el comando webcam_list se desplegarán las cámaras que estén disponibles como se observa en la figura 59.

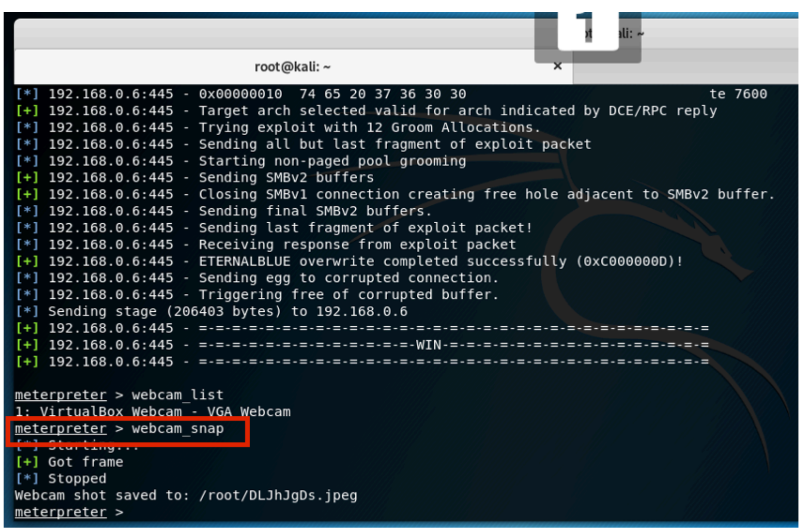
Figura 59. Revisión de cámaras disponibles



Fuente: Autor

Se procede con la ejecución del comando webcam_snap con lo que se consigue la ejecución del ataque sobre el equipo, se desplegará la ruta donde se ha guardado la imagen capturada.

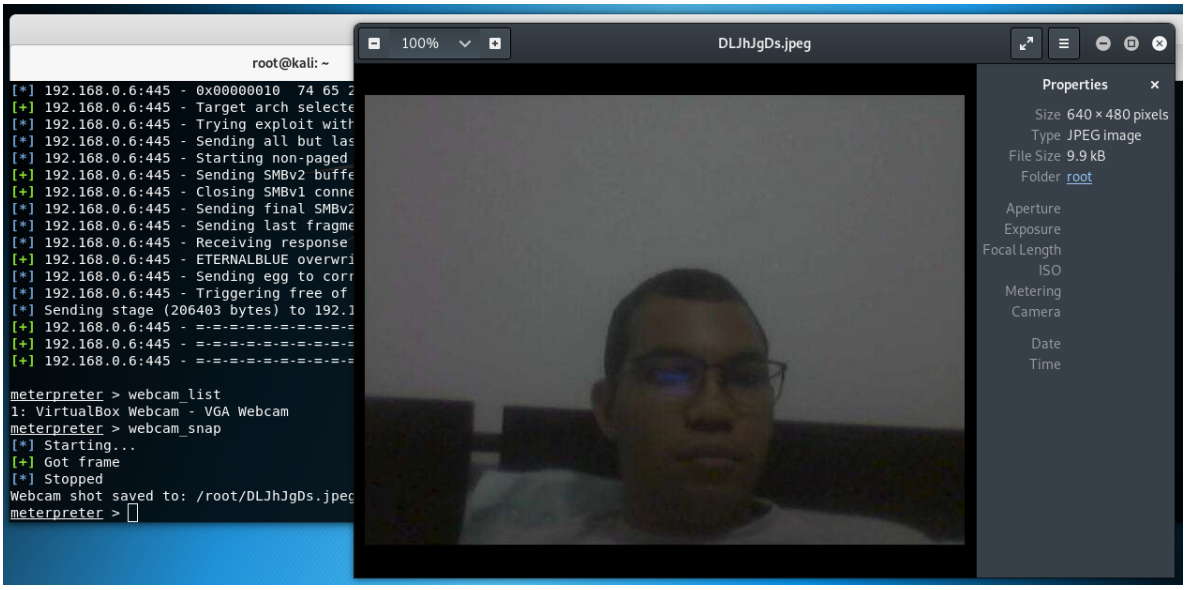
Figura 60. Ejecución de cámara web



Fuente: Autor

En la figura 61 se puede observar que el ataque se realizó de forma correcta, obteniendo acceso a la cámara web del equipo de forma remota.

Figura 61. Acceso a cámara web



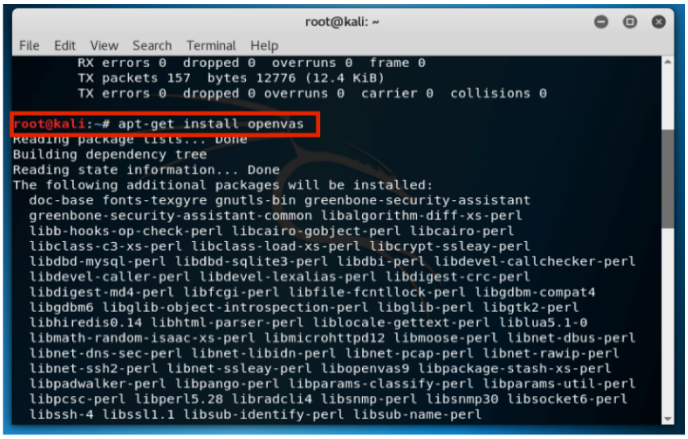
Fuente: Autor

7.2 PRUEBAS DE VULNERABILIDAD

Instalación de OpenVas

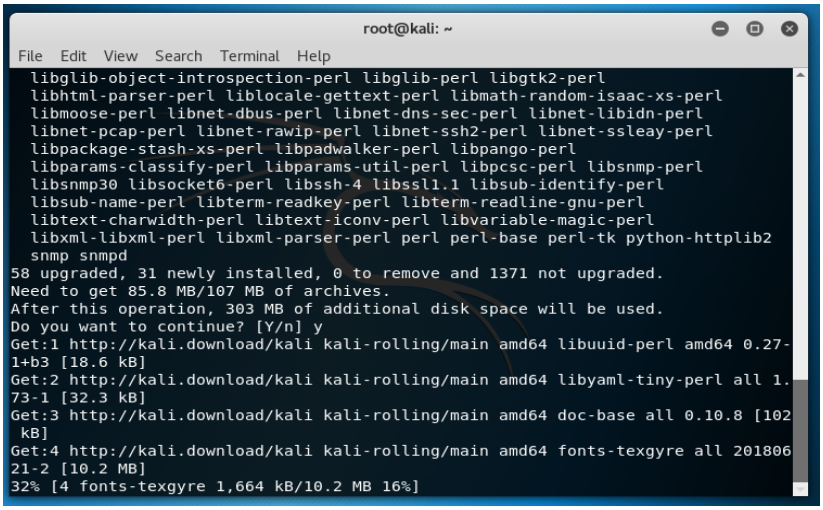
Para iniciar con la instalación, se debe abrir la ventana de terminal y ejecutar el comando apt-get install openvas, con esto se obtendrán los paquetes de instalación.

Figura 62. Instalación OpenVas



Fuente: Autor

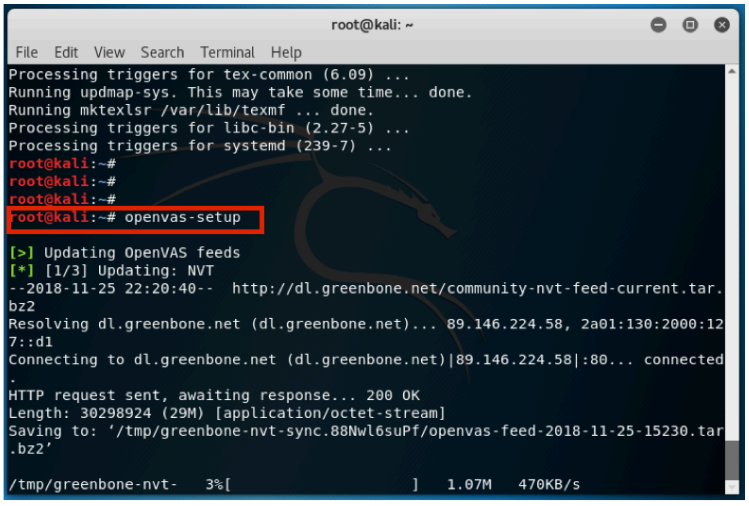
Figura 63. Progreso de instalación



Fuente: Autor

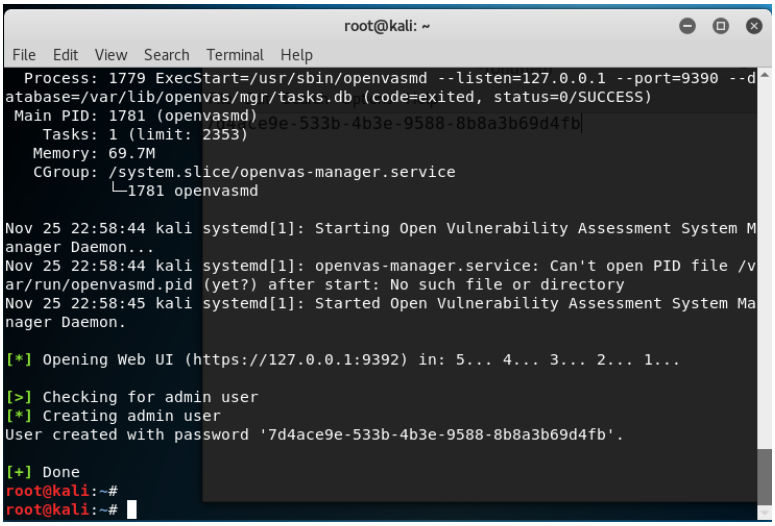
Para la configuración del *openvas* se utiliza el comando openvas-setup, una vez finalizado el proceso de instalación se obtendrá la contraseña de ingreso y el enlace para poder ingresar a la interfaz gráfica.

Figura 64. Instalación de OpenVas



Fuente: Autor

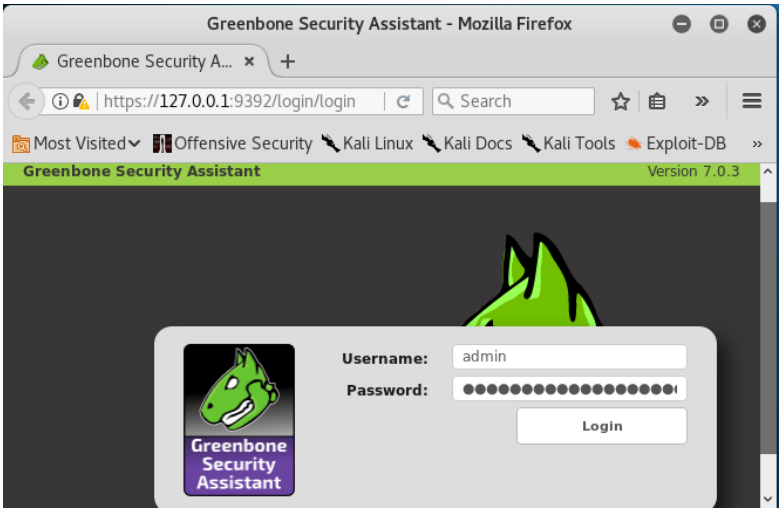
Figura 65. Finalización instalación OpenVas



Fuente: Autor

Una vez finalizado el proceso se puede ingresar a la interfaz gráfica con los datos obtenidos, se coloca en el navegador el enlace de acceso y posteriormente el usuario y la contraseña.

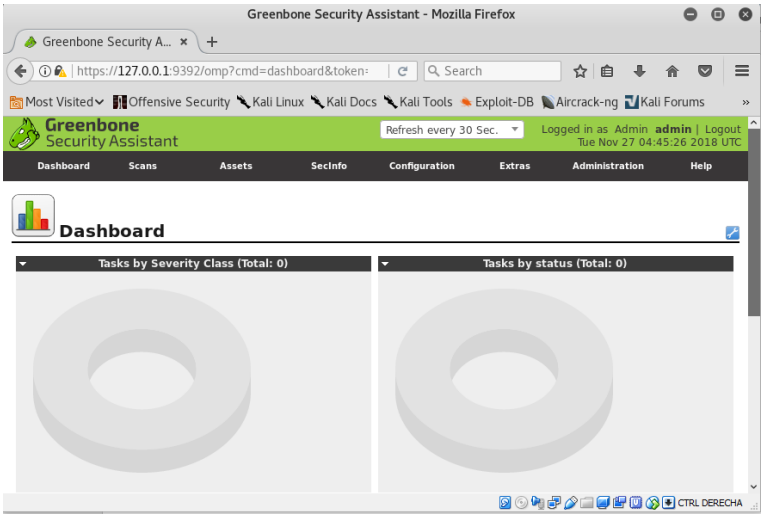
Figura 66. Ingreso a OpenVas



Fuente: Autor

Una vez se ingresa, se podrán realizar las tareas de escaneo de vulnerabilidades.

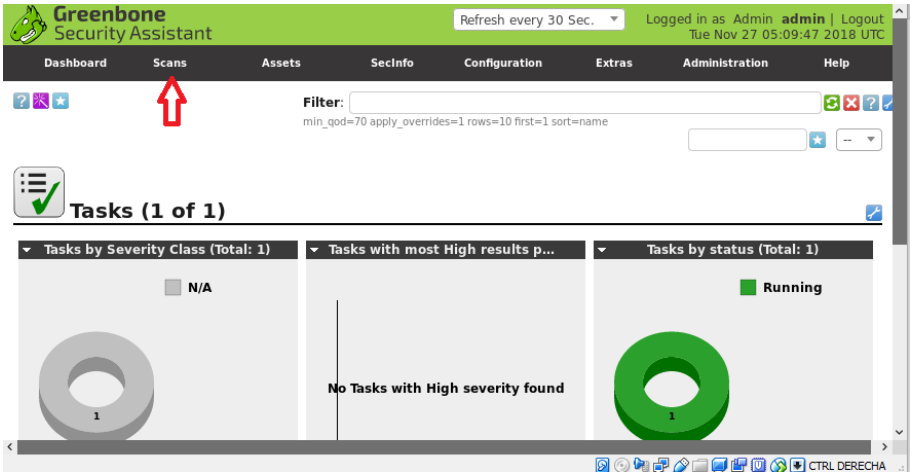
Figura 67. Página principal de OpenVas



Fuente: Autor

Ahora se procede con el inicio del proceso de escaneo de la máquina virtual con el sistema *Metasploitable*. Para ello en la parte superior se da clic sobre la pestaña *Scans* y luego se busca la opción *Task* como se observa en las figuras 68 y 69.

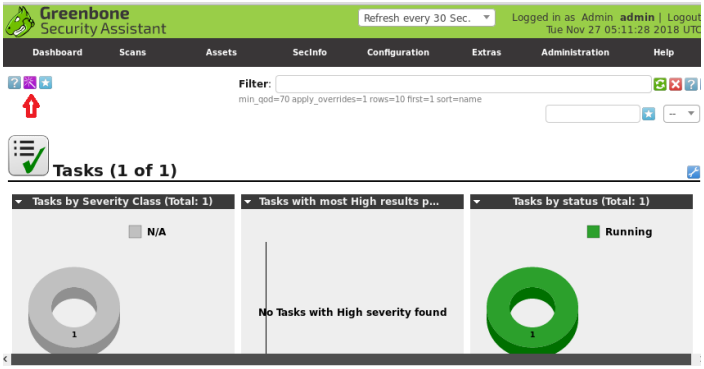
Figura 68. Ingreso a opción de escaneo



Fuente: Autor

Luego se procede a dar clic sobre *Task Wizard*, para iniciar con el proceso de exploración de las vulnerabilidades. Se desplegará la ventana donde se colocará la dirección IP de la maquina a explorar, en este caso es la máquina virtual con dirección 192.168.0.5.

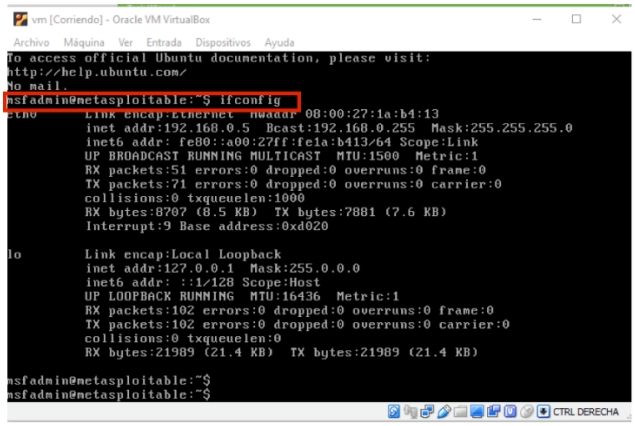
Figura 69. Ingreso al asistente de tareas



Fuente: Autor

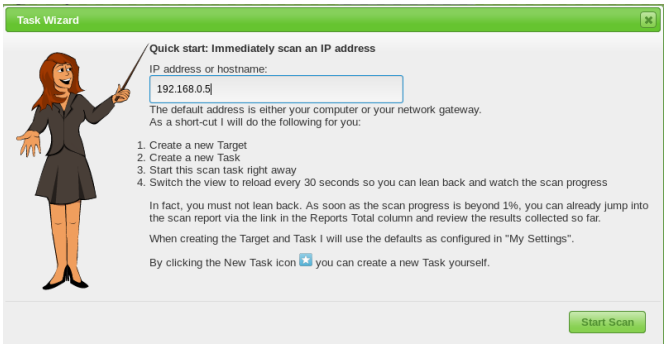
Para verificar la dirección IP sobre la cual se realizará el escaneo, en una ventana terminal sobre la máquina virtual con Linux Metasploitable se ejecuta el comando ifconfig, con el cual se obtiene el detalle de las configuraciones de red.

Figura 70. Revisión de IP del Metasploitable



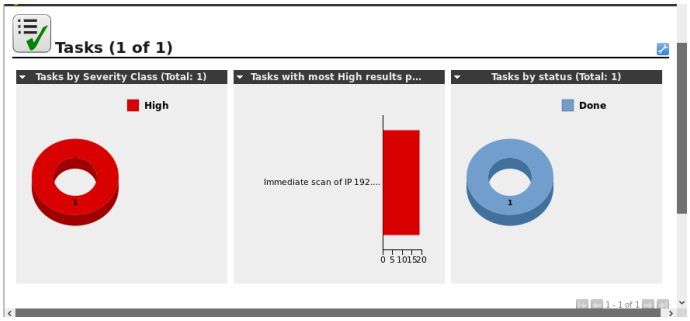
Fuente: Autor

Figura 71. Ventana Task Wizard



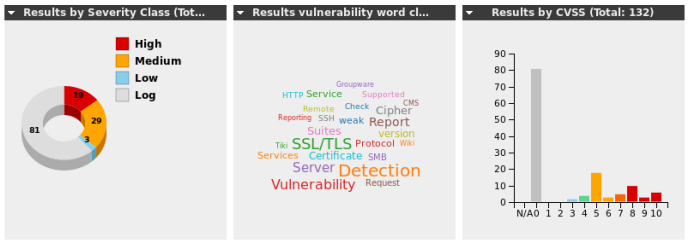
Fuente: Autor

Figura 72. Gráficas con resultados de escaneo



Fuente: Autor

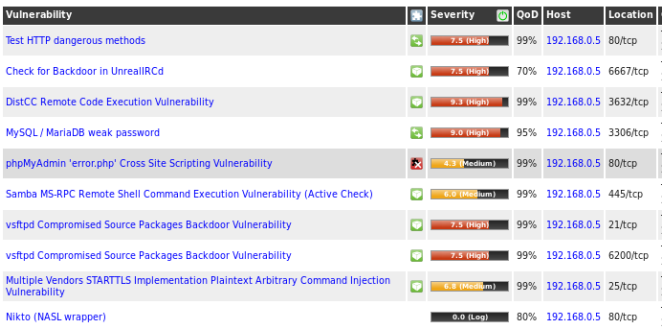
Figura 73. Gráficas con resultados de escaneo



Fuente: Autor

En la siguiente captura de pantalla se puede observar el listado de algunas de las vulnerabilidades encontradas y su nivel de severidad. Se presenta la opción de dar clic en el nombre de la vulnerabilidad, con lo cual se desplegará una nueva pestaña con las posibles correcciones a realizar.

Figura 74. Listado de vulnerabilidades encontradas



Vulnerability	Severity	QoD	Host	Location
Test HTTP dangerous methods	7.5 (High)	99%	192.168.0.5	80/tcp
Check for Backdoor in UnrealIRCd	7.5 (High)	70%	192.168.0.5	6667/tcp
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.0.5	3632/tcp
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.0.5	3306/tcp
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	4.3 (Medium)	99%	192.168.0.5	80/tcp
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0 (Medium)	99%	192.168.0.5	445/tcp
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.0.5	21/tcp
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.0.5	6200/tcp
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99%	192.168.0.5	25/tcp
Nikto (NASL wrapper)	0.0 (Log)	80%	192.168.0.5	80/tcp

Fuente: Autor

7.2.1 Descripción de Fallas de Seguridad. La tabla que se presenta a continuación detalla la descripción de 8 de las vulnerabilidades encontradas al aplicar la prueba sobre la máquina con *Metasploitable* de los ambientes controlados utilizando la aplicación Openvas.

Tabla 1. Vulnerabilidades

Nombre de la Vulnerabilidad	Descripción	Recomendación
Test HTTP *Dangerous Methods*	Esta vulnerabilidad se refiere a una mala configuración en los servidores web, permitiendo a clientes remotos ejecutar métodos de agregado de código, además de permitir su ejecución, permite al atacante también el borrado de información.	Para poder prevenir esta vulnerabilidad se deben configurar restricciones de acceso a estos métodos http o deshabilitarlos.
Check for backdoor in UnrealIRCd	Esta vulnerabilidad permite a los atacantes ejecutar código de manera sobre un equipo infectado a través de un servidor IRC	La corrección a esta vulnerabilidad consiste en instalar la última versión de *UnrealIRCd* además de revisar las firmas digitales del software a instalar.
DistCC *Remote Code Execution Vulnerability*	Cuando no se restringe el acceso a través del puerto del servidor, permite a los atacantes la ejecución de código a través de rutinas de compilación ya que estas son ejecutadas sin verificar si tienen o no autorización.	La solución consiste en la actualización del DistCC ya que la corrección es aplicada por el proveedor.

Fuente: El autor

Tabla 2. Continuación

Nombre de la Vulnerabilidad	Descripción	Recomendación
phpMyadmin error.php cross site scripting vulnerability	Esta vulnerabilidad permite el robo de credenciales de autenticación a través de cookies a usuarios de *phpMyadmin.* Para este ataque se requiere que las víctimas ejecuten un enlace con código HTML y scripts. Esta vulnerabilidad también permite la inyección de código. Este ataque se relaciona con *phishing*	Hasta la fecha no existe solución a esta vulnerabilidad, como única recomendación se tiene instalar las últimas versiones de PHPMyadmin. Afecta directamente la versión 3.3.8.1 y versiones anteriores.
Samba MS-RPC Remote Shell Command Execution Vulnerability	La funcionalidad MS-RPC en SMBD en las versiones de samba 3.0.0 a 3.0.25rc3 permite a los atacantes remotos el acceso a través del archivo smb.conf utilizando credenciales de usuarios remotos autenticados.	La solución a esta vulnerabilidad es la actualización de la versión de Samba.
Vsftpd *compromised source packages backdoor vulnerability*	Esta vulnerabilidad consiste en que se distribuyen paquetes de código fuente de puerta trasera VSFTPD, permitiendo la ejecución de código de manera remota y modificación del código fuente del software.	Se debe realizar la validación del código fuente del software, además de validar cualquier paquete de instalación a través del certificado de la firma.

Fuente: El autor

Tabla 3. Continuación

Nombre de la Vulnerabilidad	Descripción	Recomendación
SSH *brute force logins with default credentials reporting*	Esta vulnerabilidad permite a los usuarios remotos el ingreso al sistema a través del protocolo SSH, utilizando credenciales por defecto.	Utilizar contraseñas seguras o herramientas de generación de contraseñas que no permitan su fácil descifrado.
Possible Backdoor: IngresLock	A través del puerto 1524 y la utilización de unos de los servicios del sistema, se logra ingresar al sistema y ejecutar virus troyanos.	Esta vulnerabilidad se puede evitar eliminando archivos de configuración no autorizados,

Fuente: El autor

8. ANÁLISIS DE GESTIÓN DE RIESGOS

El riesgo informático es la probabilidad de que una amenaza pueda materializarse valiéndose de vulnerabilidades existentes en una organización. es una "estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización" [52].

Para garantizar la seguridad de los activos de información se debe realizar un buen análisis y una buena gestión de los riesgos, de manera que se pueda seleccionar los controles necesarios para mitigarlos o reducirlos, implementándolos de manera adecuada. El análisis de riesgo es un "proceso sistemático para estimar la magnitud de los riesgos a que se está expuesta una organización" [53], el cual tiene como objetivos, según [54](Fisher, 1988):

- Ayudar en la identificación de exposiciones.
- Ayudar en la cuantificación de los valores de las exposiciones.
- Permitir un ranking de exposiciones por prioridad.
- Servir como base para el análisis del coste eficaz.

"El análisis de riesgos determinará las amenazas y vulnerabilidades de los activos de información previamente inventariados" [55], por lo cual es fundamental en la gestión de riesgos definida como las "acciones coordinadas para dirigir y controlar una organización respecto a los riesgos" [56].

Es de suma importancia garantizar la seguridad de los sistemas informáticos y la información dentro de la organización, de tal forma que no se afecte su funcionamiento por causa de la materialización de las amenazas que puedan existir.

Es aquí donde la gestión de riesgos juega un papel muy importante en la protección de los activos, ya que permitirá realizar una adecuada selección de controles necesarios que garanticen la integridad, confidencialidad y disponibilidad de tal forma que la productividad de la organización y sus tiempos de respuesta no se vean afectados, generando pérdidas económicas para la misma.

---

[52] Dirección General de Modernización Administrativa, Procedimiento e Impulso de la Administración Electrónica. MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.
[53] Ibíd.
[54] FISHER, Royal. SEGURIDAD EN LO SISTEMAS INFORMATICOS. Madrid: Ediciones Díaz de Santos, S.A., 1988.
[55] GÓMEZ, Luis, & ÁLVAREZ, Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid: AENOR, 2012.
[56] FERNÁNDEZ, Carlos, & PIATTINI, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. Madrid: AENOR, 2012.

Aunque existen diferentes metodologías de gestión de riesgos, se decidió aplicar la metodología MAGERIT, la cual plantea los siguientes pasos y propone ciertos formatos que facilitan la realización de cada uno de estos:

- Determinación de los activos de información
- Determinación de las amenazas
- Selección de salvaguardas
- Determinación del impacto residual
- Determinación del riesgo residual

Luego de las pruebas de vulnerabilidad y los ataques realizados a los ambientes controlados de la entidad hipotética, se evidencia la necesidad de implementar los controles necesarios para evitar que la organización sea víctima de ataques que puedan explotar las vulnerabilidades encontradas. Pero antes de poder determinar estos controles, es importante llevar a cabo un análisis de riesgo que le permita a la entidad tener un panorama más amplio de los riesgos informáticos a los que se expone, para así poder contrarrestarlos y evitar daños a la organización.

8.1 DETERMINACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La determinación de los activos de información consiste en la identificación y valoración de aquellos elementos u operatividad de un sistema informático que pueden ser afectados por acciones de un sistema o una persona externa, causando daños a una organización.

8.1.1 Identificación de Activos de Información. Durante la identificación de los activos se tienen en cuenta todos aquellos que, al ser atacados, pueden causar daños a la organización, ya sean pérdida de dinero, clientes o reputación, entre otros. Para esto se tiene en cuenta la información relevante acerca de dichos activos, categorizándolos de acuerdo con la similitud que pueda existir entre ellos.

MAGERIT propone que los activos de información se agrupen en las siguientes categorías:

- [D] Datos/Información
- [K] Claves criptográficas
- [S] Servicios
- [SW] Software – Aplicaciones informáticas
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones

- [P] Personal

La siguiente tabla muestra el listado de activos identificados dentro de una entidad hipotética, en un formato propuesto por el autor que los reúne todos para facilitar su lectura. Para cado uno de ellos se detalla la siguiente información: tipo, nombre, descripción, ubicación y cantidad.

Tabla 4. Clasificación de Activos de Información

#	Tipo	Nombre	Descripción	Ubicación	Cantidad
1	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidores de Dominio	Servidor encargado de la autenticación para garantizar o denegar a un usuario el acceso a recursos de la red.	Centro de datos	2
2	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidor de impresión	Servidor encargado de gestionar las impresiones en la organización.	Centro de datos	1
3	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidor de Archivos	Servidor encargado de la gestión de archivos en la organización	Centro de datos	1
4	[AUX] EQUIPAMENTO AUXILIAR	[power] Equipos de protección eléctrica.	UPS encargada de mantener el fluído eléctrico el centro de datos	Centro de datos	1
5	[L] INSTALACIONES	[local] Centro de datos	Sitio donde se consolida los servicios de: Servidor de impresión, dominio, File server. El Centro de Cableado incluye: Sistemas de detección de incendios, aire acondicionado, control de acceso físico (Tarjeta de contacto), extintores, equipos de protección eléctrica.	Edificio entidad hipotética	1

Fuente: El Autor

Tabla 5. Continuación

#	Tipo	Nombre	Descripción	Ubicación	Cantidad
6	[SW] SOFTWARE	[std] ERP	Sistema que planifica todos los recursos empresariales de entidad hipotética	NUBE	1
7	[SW] SOFTWARE	[std] Salesforce	Aplicativo CRM que gestiona toda la relación comercial de la organización.	NUBE	1
8	[SW] SOFTWARE	[std][email_server] Correo Electrónico	Servicio de Office 365	NUBE	1
9	[COM] REDES DE COMUNICACIONES	[ipphone] Telefonía IP	Plantas telefónicas de todas las sedes, Teléfonos IP	Centro de datos - Oficinas	49
10	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – Desarrollo de negocios	PC + Sistema Operativo Windows 10, Laptop + Sistema Operativo Windows 10	Oficina Desarrollo de negocios	12
11	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – TI	PC + Sistema Operativo Windows 10, Laptop + Sistema Operativo Windows 10	Oficina de T. I	27

Fuente: El autor

Tabla 6. Continuación

#	Tipo	Nombre	Descripción	Ubicación	Cantidad
12	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – Administrativo	PC + Sistema Operativo Windows 10, Laptop + Sistema Operativo Windows 10	Oficina de Administrativo	19
13	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 60 D	Firewall perimetral que sirve para proteger las redes empresariales de ataques, *spam*, y otros peligros informáticos. Utilizado para gestión de servicios contratados por clientes	Centro de Datos	6
14	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 100 E	*Firewall* perimetral que sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos. Utilizado para gestión de servicios contratados por clientes	Centro de Datos	4

Fuente: El autor

Tabla 7. Continuación

#	Tipo	Nombre	Descripción	Ubicación	Cantidad
16	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 80E	Firewall perimetral que sirve para proteger las redes empresariales de ataques, spam, y otros peligros informáticos. Utilizado para gestión de servicios contratados por clientes	Centro de Datos	1
17	[HW] EQUIPAMENTO INFORMÁTICO	[switch] Cisco catalyst 9300	Dispositivos de red encargados de la interconexión de la red de datos	Centro de datos	3
18	[P] PERSONAL	[ui] Operadores NOC	Personal encargado de la gestión de servicios de *networking*	Oficina entidad hipotética	12
19	[SW] SOFTWARE	[std] PRTG Network Monitor	PRTG *Network Monitor* es un software de monitoreo de red sin agentes de *Paessler* AG.	Centro de Datos	1
20	[D] DATOS	Contratos de servicio	Contratos con clientes que disfrutan de los servicios brindados por la entidad hipotética	Servidor de Archivos	13

Fuente: El autor

8.1.2 Valoración de los Activos de Información. La valoración de los activos se realiza para determinar el grado de importancia que tiene cada uno dentro de una organización. El valor de un activo depende de qué tan importante sea para la organización. Entre más importante sea, mayor sería la consecuencia para una empresa si este se ve afectado. Por lo tanto, un activo con mayor valor debería tener un grado de protección mayor al interior de una organización.

Al realizar la valoración se puede utilizar cualquier escala, pero la seleccionada debe aplicarse para todas las dimensiones, de forma que se puedan comparar riesgos. La siguiente tabla muestra la escala definida por el autor para llevar a cabo la valoración de los activos de información de la entidad hipotética, esta escala contiene valores cuantitativos y cualitativos.

Tabla 8. Escala para la valoración de los activos

VALOR		CRITERIO
MA	5	daño muy grave
A	4	daño grave
M	3	daño importante
B	2	daño menor
MB	1	irrelevante a efectos prácticos

Fuente: El autor

En la siguiente tabla se detalla la valoración tanto cuantitativa realizada a los diferentes activos de información de la entidad hipotética. Esta valoración se realizó para las siguientes dimensiones de la seguridad de la información: autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad.

Tabla 9. Valoración de activos

#	TIPO	NOMBRE	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR TOTAL
1	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidores de Dominio	5	3	5	2	5	4
2	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidor de impresión	1	1	3	2	4	2

Fuente: El autor

Tabla 10. Continuación

#	TIPO	NOMBRE	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR TOTAL
3	[HW] EQUIPAMENTO INFORMÁTICO	[host] Servidor de Archivos	4	3	5	5	5	4
4	[AUX] EQUIPAMENTO AUXILIAR	[power] Equipos de protección eléctrica.	1	1	1	5	5	3
5	[L] INSTALACIONES	[local] Centro de datos	5	5	5	5	5	5
6	[SW] SOFTWARE	[std] ERP	5	5	5	5	3	5
7	[SW] SOFTWARE	[std] SalesForce	3	3	5	4	3	4
8	[SW] SOFTWARE	[std][email_server] Correo Electrónico	5	5	5	5	2	4
9	[COM] REDES DE COMUNICACIONES	[ipphone] Telefonía IP	2	2	2	4	5	3
10	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – Desarrollo de negocios	4	4	5	4	5	4
11	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – TI	5	5	5	5	5	5
12	[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipos de cómputo de los usuarios finales – Administrativo	5	5	5	5	5	5
13	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 60 D	2	4	4	5	5	4
14	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 100 E	2	4	4	5	5	4
15	[HW] EQUIPAMENTO INFORMÁTICO	[wap] FortiAP 24d	2	2	2	4	5	3
16	[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Fortigate 80E	2	4	4	5	5	4
17	[HW] EQUIPAMENTO INFORMÁTICO	[switch] Cisco catalyst 9300	2	2	2	5	5	3

Fuente: El autor

Tabla 11. Continuación

#	TIPO	NOMBRE	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR TOTAL
18	[P] PERSONAL	[ui] Operadores NOC	5	5	4	5	5	5
19	[SW] SOFTWARE	[std] PRTG Network Monitor	3	5	3	5	5	4
20	[D] DATOS	Contratos de servicio	5	2	5	5	2	4

Fuente: El autor

8.2 DETERMINACIÓN DE LA AMENAZAS

La determinación de las amenazas consiste en la identificación y valoración de aquello que puede causar daños a los activos de información de una organización. Durante la valoración se tiene en cuenta el impacto que pueda tener la materialización de la amenaza sobre un activo de información, esto es, qué tan perjudicado se pueda ver el valor de un activo. Adicionalmente, se tiene en cuenta la probabilidad de que se materialicen amenazas en la organización.

MAGERIT propone clasificar las amenazas que pueden sufrir los activos de información en los siguientes cuatro grupos:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores o fallos no intencionados
- [A] Ataques intencionados

Para cada una de las amenazas se define el impacto sobre cada uno de los activos y la probabilidad de que estas se materialicen. Las tablas 5 y 6 muestran las escalas definidas por los autores para llevar a cabo la evaluación de las amenazas a las que se ven expuestos los activos de información de la organización.

Tabla 12. Escala de Impacto

Nomenclatura	Categoría	Valoración
MA	Muy Alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy Bajo	1

Fuente: El autor

Tabla 13. Escala de probabilidad

Nomenclatura	Categoría	Valoración
MA	Prácticamente seguro	5
A	Probable	4
M	Posible	3
B	Poco probable	2
MB	muy raro	1

Fuente: El autor

Luego de definir la escala para valorar el impacto y la probabilidad, se procede a realizar el cálculo del riesgo para cada uno de los activos, el cual será dado por la siguiente fórmula: *R* = *Valor Activo* x *Impacto* x *Probabilidad*

Tabla 14. Cálculo del riesgo

Nombre del activo de información	Amenazas	Valoración activos	Impacto	Probabilidad	Cálculo del riesgo neto
[host] Servidores de Dominio	[I1] Fuego	4	5	3	60
[host] Servidor de impresión	[I1] Fuego	1	5	3	15
[host] Servidor de Archivos	[A18] Destrucción de información	4	4	5	80
[power] Equipos de protección eléctrica.	[I1] Fuego	1	5	3	15

Fuente: El autor

Tabla 15. Continuación

Nombre del activo de información	Amenazas	Valoración activos	Impacto	Probabilidad	Cálculo del riesgo neto
[local] Centro de datos	[I1] Fuego	5	5	3	75
[std] ERP	[I8] Fallo de servicios de comunicaciones	5	3	4	60
[std] SalesForce	[I8] Fallo de servicios de comunicaciones	3	3	4	36
[std][email_server] Correo Electrónico	[I8] Fallo de servicios de comunicaciones	5	3	4	60
[ipphone] Telefonía IP	[E25] Pérdida de equipos	2	2	4	16
[pc] Equipos de cómputo de los usuarios finales – Desarrollo de negocios	[E25] Pérdida de equipos	4	3	4	48
[pc] Equipos de cómputo de los usuarios finales – TI	[E25] Pérdida de equipos	5	3	4	60
[pc] Equipos de cómputo de los usuarios finales – Administrativo	[E25] Pérdida de equipos	5	3	4	60
[firewall] Fortigate 60 D	[E21] Errores de mantenimiento / actualización de programas (software)	4	4	4	64
[firewall] Fortigate 100 E	[E4] Errores de configuración	4	4	5	80
[wap] FortiAP 24d	[E9] Errores de [re-]encaminamiento	2	3	4	24

Fuente: El autor

Tabla 16. Continuación

Nombre del activo de información	Amenazas	Valoración activos	Impacto	Probabilidad	Cálculo del riesgo neto
[firewall] Fortigate 80E	[E20] Vulnerabilidades de los programas (software)	4	4	4	64
[switch] Cisco catalyst 9300	[E9] Errores de [re-]encaminamiento	2	3	4	24
[ui] Operadores NOC	[A19] Divulgación de información	5	3	4	60
[std] PRTG Network Monitor	[E3] Errores de monitorización (log)	4	3	5	60
Contratos de servicio	[A15] Modificación deliberada de la información	3	3	4	36

Fuente: El autor

8.3 SELECCIÓN DE SALVAGUARDAS

En esta etapa se realiza la identificación de aquellas salvaguardas que se encuentran implementadas en la organización, valorando su efectividad ante las diferentes amenazas a las que está expuesta. MAGERIT propone diferentes salvaguardas, las cuales se encuentran agrupadas en 16 categorías:

- Protecciones generales u horizontales
- Protección de los datos / información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección en los puntos de interconexión con otros sistemas
- Protección de los soportes de información
- Protección de los elementos auxiliares
- Seguridad física – Protección de las instalaciones
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo
- Continuidad de operaciones
- Externalización

- Adquisición y desarrollo

Para valorar las salvaguardas para cada uno de los activos, se define la siguiente escala de calificación de gestión:

Tabla 17. Escala de valoración de salvaguardas

Categoría	Valoración
Efectivo y documentado	4
Efectivo, pero no documentado	3
Existe, pero no efectivo	2
Control no existe	1

Fuente: El autor

Riesgo residual

Luego de identificar y valorar las salvaguardas existentes en la empresa para cada uno de los activos, se realiza el cálculo del riego residual, para el cual se aplica la fórmula: *Riesgo Residual = Riesgo / Valor Salvaguarda*

La siguiente tabla relaciona cada uno de los activos identificados en la entidad hipotética, las amenazas, el riesgo, la calificación de la salvaguarda, la salvaguarda o control y el cálculo del riesgo residual.

Tabla 18. Identificación y evaluación de salvaguardas

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
1	[host] Servidores de Dominio	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires	4	5	3	60	2	Mantenimiento de aires acondicionados en centro de datos	30
2	[host] Servidor de impresión	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires	1	5	3	15	2	Mantenimiento de aires acondicionados en centro de datos	7,5
3	[host] Servidor de Archivos	[A18] Destrucción de información	Eliminación de la información por inconformidad de los usuarios	4	4	5	80	1	Copias de seguridad de los datos (*backup*)	80

Fuente: El autor

Tabla 19. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
4	[power] Equipos de protección eléctrica.	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires	1	5	3	15	2	Mantenimiento de aires acondicionados en centro de datos	7,5
5	[local] Centro de datos	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires	5	5	3	75	2	Mantenimiento de aires acondicionados en centro de datos	37,5
6	[std] ERP	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio	5	3	4	60	2	Adquisición de canal dedicado de internet de 10 MB	30

Fuente: El autor

Tabla 20. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
7	[std] SalesForce	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio	3	3	4	36	2	Adquisición de canal dedicado de internet de 10 MB	18
8	[std][email_server] Correo Electrónico	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio	5	3	4	60	2	Adquisición de canal dedicado de internet de 10 MB	30
9	[ipphone] Telefonía IP	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas	2	2	4	16	1	Control de acceso físico	16

Fuente: El autor

Tabla 21. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
10	[pc] Equipos de cómputo de los usuarios finales – Desarrollo de negocios	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de Desarrollo de negocios y falta de control de ingreso de personal externo a la organización	4	3	4	48	1	Control de acceso físico	24
11	[pc] Equipos de cómputo de los usuarios finales – TI	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de TI y falta de control de ingreso de personal externo a la organización	5	3	4	60	1	Control de acceso físico	60

Fuente: El autor

Tabla 22. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
12	[pc] Equipos de cómputo de los usuarios finales – Administrativo	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de Administrativo y falta de control de ingreso de personal externo a la organización	5	3	4	60	1	Control de acceso físico	60
13	[firewall] Fortigate 60 D	[E21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento por falta de licencia de uso	4	4	4	64	2	Configuración del Firewall perimetral	32

Fuente: El autor

Tabla 23. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
14	[firewall] Fortigate 100 E	[E4] Errores de configuración	Mal funcionamiento por faltas de reglas de autorización y denegación de transmisión y comunicación	4	4	5	80	2	Configuración del Firewall perimetral	40
15	[wap] FortiAP 24d	[E9] Errores de [re-]encaminamiento	Mal funcionamiento por falta de documentación de la segmentación de la red	2	3	4	24	3	Separación de las redes	8

Fuente: El autor

Tabla 24. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
16	[firewall] Fortigate 80E	[E20] Vulnerabilidades de los programas (software)	Mal funcionamiento por falta de licencia de uso	4	4	4	64	2	Configuración del Firewall perimetral	32
17	[switch] Cisco catalyst 9300	[E9] Errores de [re-]encaminamiento	Mal funcionamiento por falta de documentación de la segmentación de la red	2	3	4	24	3	Separación de las redes	12

Fuente: El autor

Tabla 25. Continuación

#	Nombre Activo	Amenaza	Riesgo	Valoración	Impacto	Probabilidad	Cálculo del riesgo	Calificación de gestión de la salvaguarda	Control	Riesgo Residual
18	[ui] Operadores NOC	[A19] Divulgación de información	Fuga de información de los funcionarios por falta de requerimientos de seguridad de la Ley 1581 de 2012 de protección de datos personales	5	3	4	60	1	Cifrado de la información	60
19	[std] PRTG Network Monitor	[E3] Errores de monitorización (log)	Mal funcionamiento por controles de navegación insuficientes	4	3	5	60	1	Herramienta de monitorización de tráfico	60
20	Contratos de servicio	[A15] Modificación deliberada de la información	Alteración de la información por inconformidad de los empleados	3	3	4	36	1	Aseguramiento de la integridad	36

Fuente: El autor

Pan de tratamiento de riesgos

Tabla 26. Plan de tratamiento de riesgos

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[host] Servidores de Dominio	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires		X		A11.2.4	Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.
[host] Servidor de impresión	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires		X		A11.2.4	Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Fuente: El autor

Tabla 27. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[host] Servidor de Archivos	[A18] Destrucción de información	Eliminación de la información por inconformidad de los usuarios			X	A.8.1.4	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo
[power] Equipos de protección eléctrica.	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires		X		A11.2.4	Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Fuente: El autor

Tabla 28. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[local] Centro de datos	[I1] Fuego	Daño de aires por falta de mantenimiento preventivo de aires		X		A11.2.4	Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.
[std] ERP	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio		X		A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Fuente: El autor

Tabla 29. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[std] SalesForce	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio		X		A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
[std][email_server] Correo Electrónico	[I8] Fallo de servicios de comunicaciones	Indisponibilidad del servicio		X		A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

Fuente: El autor

Tabla 30. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[ipphone] Telefonía IP	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas		X		A9.1.1	Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
[pc] Equipos de cómputo de los usuarios finales – Desarrollo de negocios	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de Desarrollo de negocios y falta de control de ingreso de personal externo a la organización			X	A9.1.1	Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

Fuente: El autor

Tabla 31. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[pc] Equipos de cómputo de los usuarios finales – TI	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de TI y falta de control de ingreso de personal externo a la organización			X	A9.1.1	Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
[pc] Equipos de cómputo de los usuarios finales – Administrativo	[E25] Pérdida de equipos	Robo de equipos por falta de sistema de control de acceso en oficinas de Administrativo y falta de control de ingreso de personal externo a la organización			X	A9.1.1	Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

Fuente: El autor

Tabla 32. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[firewall] Fortigate 60 D	[E21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento por falta de licencia de uso		X		A13.1.1	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
[firewall] Fortigate 100 E	[E4] Errores de configuración	Mal funcionamiento por faltas de reglas de autorización y denegación de transmisión y comunicación		X		A13.1.1	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
[wap] FortiAP 24d	[E9] Errores de [re-]encaminamiento	Mal funcionamiento por falta de documentación de la segmentación de la red		X			

Fuente: El autor

Tabla 33. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[firewall] Fortigate 80E	[E20] Vulnerabilidades de los programas (software)	Mal funcionamiento por falta de licencia de uso		X		A13.1.1	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
[switch] Cisco catalyst 9300	[E9] Errores de [re-]encaminamiento	Mal funcionamiento por falta de documentación de la segmentación de la red		X			
[ui] Operadores NOC	[A19] Divulgación de información	Fuga de información de los funcionarios por falta de requerimientos de seguridad de la Ley 1581 de 2012 de protección de datos personales			X	A8.1.3	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información

Fuente: El autor

Tabla 34. Continuación

Nombre activo de información	Amenazas Metodología Magerit	Riesgo	Transferir	Aceptar	Mitigar	Control aplicar a partir de la norma ISO 27001	Descripción de la aplicación del control
[std] PRTG Network Monitor	[E3] Errores de monitorización (log)	Mal funcionamiento por controles de navegación insuficientes			X	A9.1.2	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar
Contratos de servicio	[A15] Modificación deliberada de la información	Alteración de la información por inconformidad de los empleados		X			

Fuente: El autor

9. PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

9.1 SITUACIÓN ACTUAL

La entidad hipotética cuenta con tres dependencias, Desarrollo de Negocios, T.I y Administrativo, las cuales se dividen en los diferentes departamentos encargados de realizar las diferentes actividades para el funcionamiento de la organización. A continuación, se presenta el organigrama actual de la entidad hipotética.
Figura 75 Organigrama actual de la organización

Fuente: El autor

Adicionalmente, en la entidad hipotética se presentan las siguientes situaciones, las cuales ponen en riesgo la confidencialidad, disponibilidad e integridad de los activos de información de la entidad hipotética:

- La entidad no cuenta con un Sistema de Gestión de Seguridad de la información.
- El centro de datos es el único que cuenta con acceso con tarjeta de proximidad.
- El centro de datos cuenta con 2 aires acondicionados mini Split de 1200 BTU y se les hace mantenimiento preventivo 1 vez al año.
- En los últimos 2 años se han generado pérdida de datos debido a empleados inconformes.
- La segmentación de la RED no se ha documentado por lo cual cada vez que hay un inconveniente se debe invertir mucho tiempo en su resolución.

- El ingreso de personal externo a la organización no se controla de manera adecuada.
- Los equipos *Fortigate* internos de la compañía no tienen reglas definidas ni licencia de uso.
- La organización cuenta con un canal dedicado de internet de 10 MB.
- Los computadores portátiles no cuentan con cifrado en disco duro.
- La organización no cumple con los requerimientos de seguridad de la Ley 1581 de 2012 de protección de datos personales.
- Los controles de navegación son insuficientes para las necesidades de la organización.

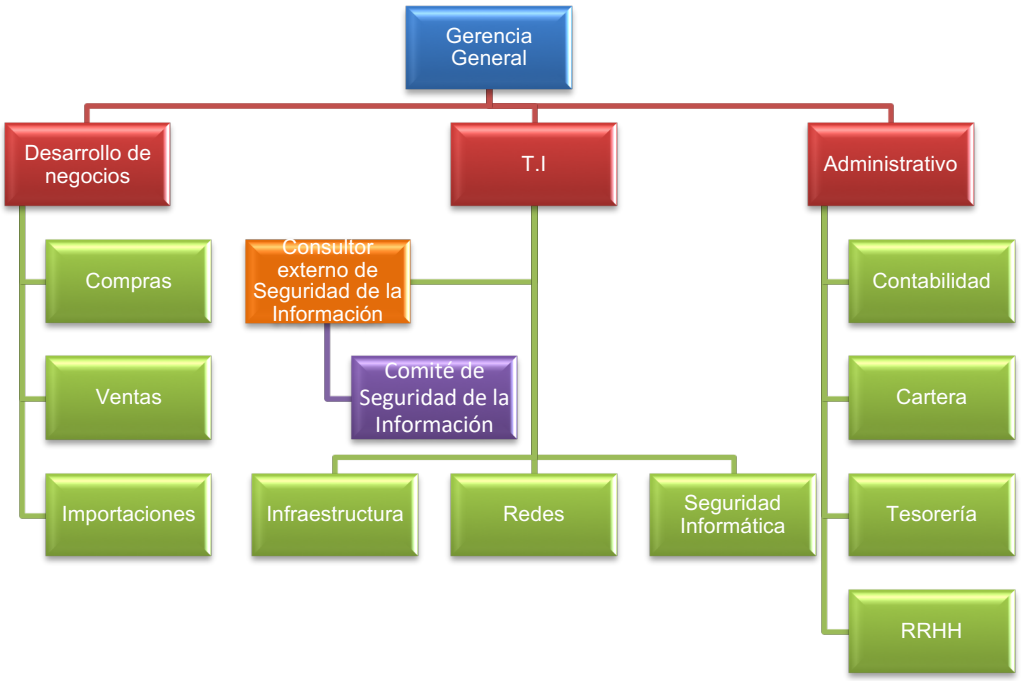
9.2 CAMBIO ORGANIZACIONAL

Previo al diseño del plan estratégico de seguridad de la información en la entidad hipotética, se debe realizar la contratación de un consultor externo de Seguridad de la Información que apoye y guíe a la empresa en el aseguramiento de los activos de información. Luego de la contratación del consultor externo de Seguridad de la Información se propone reorganizar la estructura organizacional de la siguiente forma:

Agregar al consultor de Seguridad de la Información como apoyo al área de T.I y el comité de Seguridad de la Información como dependiente del consultor para la correcta implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información. Es relevante que el consultor y el comité se encuentren dentro de la estructura organizacional para que la empresa tome conciencia de la importancia de la Seguridad de la Información en el funcionamiento de esta, con el fin de cumplir con los objetivos estratégicos propuestos por la alta dirección.

La siguiente imagen ilustra la estructura organizacional propuesta para la entidad hipotética, donde se evidencia la adición del consultor y la conformación del comité de seguridad de la información.

Figura 76 Organigrama propuesto de la organización



Fuente: El autor

9.3 REESTRUCTURACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El comité de Seguridad de la Información existente en la empresa hipotética no cuenta con la visibilidad necesaria dentro de la organización y no se está cumpliendo la realización de las sesiones periódicas de acuerdo con lo planeado. Debido a esto se propone realizar una reestructuración del comité involucrando a directivos de otras áreas de la organización y definiendo la periodicidad de las sesiones, con el fin de garantizar el cumplimiento del plan estratégico trazado por la alta dirección.

A continuación, se establecen los participantes del comité, sus funciones dentro del comité, las responsabilidades del comité, las funciones que debe llevar a cabo el consultor de Seguridad de la Información dentro del comité y la periodicidad de las sesiones ordinarias y extraordinarias.

Tabla 35. Miembros del comité de Seguridad de la Información y sus funciones

INTEGRANTES	FUNCIONES
Director de TI	• Tomar decisiones acerca de las acciones planteadas por el comité en cuanto a los proyectos de seguridad de la información. • Concientizar a los miembros del área de TI acerca de las decisiones tomadas en el comité. • Disponer de los recursos tecnológicos para la implementación del Sistema de Gestión de Seguridad de la información.
Director de Desarrollo de Negocios	• Tomar decisiones acerca de las acciones planteadas por el comité en cuanto a los proyectos de seguridad de la información. • Concientizar a los miembros del área de TI acerca de las decisiones tomadas en el comité. • Validar la documentación del Sistema de Gestión de Seguridad de la Información con los dueños de los procesos en el área de Desarrollo de negocios
Director Administrativo	• Tomar decisiones acerca de las acciones planteadas por el comité en cuanto a los proyectos de seguridad de la información. • Concientizar a los miembros del área de TI acerca de las decisiones tomadas en el comité. • Validar la documentación del Sistema de Gestión de Seguridad de la Información con los dueños de los procesos en el área de Desarrollo de negocios

Fuente: El autor

Tabla 36. Continuación

INTEGRANTES	FUNCIONES
Consultor Externo de Seguridad Informática	• Dar continuidad a la gestión de la estrategia de seguridad de la información para continuar apoyando al responsable de ciber seguridad una vez sea contratado. • Mantener la alineación de los objetivos de seguridad de la información con los objetivos del área, desarrollando el plan estratégico de seguridad PESI. • Continuar desarrollando la cultura organizacional en seguridad de la información y protección de datos personales. • Mantener el cumplimiento regulatorio relacionado con la seguridad y privacidad de la información. • Evaluar el nivel de seguridad y de exposición de activos a través de análisis de riesgos, vulnerabilidades, pruebas de intrusión y de ingeniería social, además de apoyar la remediación de las vulnerabilidades y brechas encontradas a través de esas actividades.
Oficial de Seguridad de la Información	• Establecer, implementar y mantener el Sistema de Gestión de Seguridad de la Información • Realizar el análisis de riesgos de seguridad de la información. • Definir del plan de tratamiento de los riesgos. • Ejecutar el plan de tratamiento de los riesgos • Establecer, mantener y divulgar las políticas, procedimientos y formatos del SGSI. • Informar al comité de Seguridad de la Información acerca de incidentes que pongan en riesgo la implementación del SGSI
Secretaría Técnica	• Realizar las actas de las reuniones del Comité • Convocar a los miembros del Comité a las sesiones ordinarias o extraordinarias • Agendar las sesiones oportunamente en el calendario a los del comité. • Monitorear compromisos y tareas pendientes del Comité.

Fuente: El autor

Responsabilidades del Comité de Seguridad de la Información:

- Impulsar la implementación del Sistema de Gestión de Seguridad de la Información al interior de la organización.
- Establecer el estado actual de la seguridad de la información en la entidad hipotética
- Realizar el acompañamiento e impulsar proyectos de seguridad de la información dentro de la organización.
- Participar en el proceso de identificación, evaluación y tratamiento de riesgos.
- Definir los niveles de riesgos aceptables.
- Aprobar el plan de tratamiento de riesgos de Seguridad de la Información.
- Realizar revisiones periódicas del SGSI, la cual se llevará a cabo anualmente, y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la organización.

Reuniones del comité de Seguridad de la Información:

- **Ordinaria**: El comité de Seguridad de la Información deberá llevar a cabo reuniones ordinarias una vez cada 6 meses.
- **Extraordinaria**: El comité de Seguridad de la información se reunirá de forma extraordinaria cuando el director de TI lo requiera y siempre que se presenten incidentes de seguridad o haya nuevas necesidades de seguridad.

9.4 IMPORTANCIA DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

El plan estratégico de seguridad de la información (PESI) tiene como objetivo definir los proyectos que se llevarán a cabo dentro de la organización que permitan proteger sus activos de información. Es importante crear un PESI en la entidad hipotética debido a que se encuentra en proceso de crecimiento y expansión de sus servicios para grandes compañías en el país, por lo que se hace necesario mejorar la seguridad en todos los aspectos relacionados con la prestación de sus servicios.

Teniendo en cuenta el estado actual de la compañía, se hace indispensable realizar la planeación de los proyectos que se deben llevar a cabo dentro de la organización para garantizar la integridad, confidencialidad y disponibilidad de los activos de información, lo que conllevará a ofrecer un mejor servicio a sus clientes, garantizando la calidad de estos.

9.5 OBJETIVOS Y ALCANCE DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Objetivo General

Establecer la estrategia de Seguridad de la Información en la entidad hipotética, guiada por el departamento de TI, que permita garantizar la integridad, confidencialidad y disponibilidad de los activos de información, con vigencia a partir del 2019 hasta el 2023.

Objetivos Específicos

- Implementar y mantener el Sistema de Gestión de la Seguridad de la Información.
- Desarrollar la cultura organizacional en seguridad de la información y protección de datos personales
- Cumplir las regulaciones relacionadas con la seguridad y privacidad de la información
- Utilizar eficientemente los recursos de TI para asegurar la continuidad de la prestación de los servicios
- Implantar la estrategia de Seguridad de la información

Alcance

El alcance del plan estratégico de Seguridad de la Información se aplica a los servicios de configuración e instalación de dispositivos de red y gestión de servicios telemáticos ofrecidos por la entidad hipotética.

9.6 DEFINCIÓN DE PROYECTOS DE SEGURIDAD

Una vez analizado el estado actual de la compañía por parte de la Dirección de T.I. y de acuerdo con el análisis y evaluación de los riesgos se determinó que debido al gran crecimiento en 2019 y alineado con los servicios que se prestan, es necesario para poder mantener la línea de crecimiento priorizar sobre los siguientes proyectos:

Tabla 37. Proyectos de seguridad

Nombre del Proyecto	Tiempo de Ejecución	Plazo
Sistema de Gestión de Seguridad de la Información (SGSI).	12 meses	Mediano
Seguridad Perimetral	6 meses	Corto

Fuente: El autor

9.6.1 Sistema de Gestión de Seguridad de la Información De acuerdo con las oportunidades de mejora encontradas en la entidad hipotética, el objetivo principal es garantizar los aspectos relevantes de la seguridad de la información, es decir su disponibilidad, integridad y confidencialidad.

La protección de información sensible es esencial para mantener los niveles de competitividad, rentabilidad e imagen empresarial, siempre necesarios en la búsqueda de lograr los objetivos organizacionales y asegurar de la misma forma beneficios económicos que permitan el crecimiento.

Para el diseño del SGSI es necesario tener en cuenta los siguientes aspectos:

Compromiso y apoyo de la dirección, esto debe ser traducido en

- Establecimiento de una política de seguridad de la información.
- Establecer objetivos y planes del SGSI.
- Establecimiento de roles y responsabilidades de la seguridad de la información.
- La organización debe estar al tanto de la importancia del logro de los objetivos de la seguridad de la información, del cumplimiento de las políticas, responsabilidades legales y la necesidad de mejora continua.
- Asignación de recursos suficientes al SGSI.
- Plantear cuáles serán los criterios para la aceptación de los riesgos.

Definición del alcance

Concientización y formación del personal

- Se debe determinar cuáles serán las competencias del personal que ayudará en el diseño e implementación del SGSI.
- Realizar contratación de asesores en caso de ser necesitado.
- Garantizar que todo el personal involucrado en el proceso esté concientizado de la importancia de las actividades asignadas con respecto a la seguridad de la información y de cómo estas ayudan a la consecución de los objetivos del SGSI

Realizar una evaluación de riesgos acorde con la organización.

Asumir compromisos de mejora por parte de la dirección,

- Revisión del SGSI de manera periódica con el fin de asegurar que aún es adecuado y eficaz.

Establecer normas y políticas.

Realizar una gestión adecuada de la continuidad del negocio, incidentes de seguridad y el cumplimiento legal.

Integrar el SGSI a la organización.

Factores de Éxito

- El primer objetivo por conseguir es la concientización del trabajador acerca de la importancia de la seguridad de la información.
- Reuniones periódicas para la gestión continua del SGSI.
- Crear un sistema de gestión de incidencias que permita recoger incidencias reportadas por los usuarios de manera continua.
- Se debe tener en cuenta que ningún sistema es 100% seguro, sin embargo, es posible llevar el riesgo a niveles que puedan ser asumidos.
- La seguridad no debe ser vista como un producto sino como un proceso.
- La seguridad no debe ser vista como un proyecto sino como una actividad que debe ser realizada de manera continua, para lo cual se requiere el apoyo de la organización para poder tener éxito.
- La seguridad siempre debe hacer parte de los procesos de información y alineada al negocio.

9.6.2 Seguridad Perimetral: La seguridad perimetral debe ir alineada a una política de cumplimiento de controles basado en una norma aplicada a la seguridad de la información, en este caso la ISO/IEC 27001 la cual va dirigida a procesos, activos y riesgos, todos ellos pertenecientes al área de T.I.

Se debe definir un esquema de seguridad que permita garantizar que las personas solo tengan acceso a sistemas y servicios autorizados de acuerdo con su perfil, así mismo este esquema debe permitir la mitigación de riesgos asociados con las conexiones con redes públicas, internas o de proveedores de servicio.

La seguridad perimetral debe comprender los siguientes aspectos:

- Gestión de acceso e identidad.
- Seguridad en el puesto de trabajo.
- Seguridad en aplicaciones y datos.
- Seguridad en los sistemas donde se aloja la información.
- Seguridad en las redes.

10. CONCLUSIONES

A partir de la recreación de las configuraciones y topología de red pertenecientes a la empresa hipotética en su sede en Bogotá y evidenciar las vulnerabilidades que albergaban los sistemas de información, se puede concluir a partir de los hallazgos, la importancia de la seguridad informática, y como con la realización de buenas prácticas se pueden disminuir los riesgos ante amenazas cibernéticas.

Es importante tener siempre presente la información como activo fundamental de todas las compañías, por ello al momento de pensar en la implementación de sistemas de seguridad, se debe realizar un análisis previo de gestión de riesgo, alineado con el plan estratégico de la seguridad que permita identificar cuáles son los riesgos asociados a los sistemas de información de la organización y como mitigarlos.

Así mismo, para lograr el éxito en la implementación de un plan de gestión de seguridad informática, es necesario apoyarse en estándares internacionales como guía, que ayuden con la elaboración de un plan de acción, al igual que en metodologías como Magerit las cuales ayudan a comprender como mitigar un riesgo a partir de la posibilidad de que este suceda.

11. RECOMENDACIONES

Dada la importancia de los activos de información en una organización, resulta indispensable la implementación de un plan estratégico de la seguridad de la información (PESI), de acuerdo con el análisis llevado a cabo y los hallazgos encontrados en el desarrollo de este proyecto se realizan las siguientes recomendaciones:

La información es el activo más importante de la empresa, por tal motivo, siempre debe existir un plan estratégico de la seguridad de la información, previo a la implementación de este, se debe realizar un análisis de los riesgos asociados a los sistemas de información, de tal manera que se cobije en caso de ocurrencia su mitigación.

La elaboración del plan estratégico de la seguridad de la información debe estar soportado por estándares y normas internacionales que ayuden a garantizar el éxito de este, como por ejemplo la ISO 27002.

En necesario un monitoreo constante de los controles establecidos sobre los sistemas de información, para ello se sugiere la planificación de auditorías de manera periódica que ayuden a garantizar la eficacia de estos.

BIBLIOGRAFÍA

AGUILERA, Purificación. 2010. Seguridad Informática. Madrid: Editorial Editex, S.A, 2010. 9p

AGUILERA, Purificación. 2011. Políticas de almacenamiento y resguardo de la información, p.194. Madrid: Editex.

ALEGRE, María y GARCÍA, Alfonso. Seguridad Informática Ed.11. España: Paraninfo, 2011. 2p.

ALEJANDRO. Utilidad para testear la vulnerabilidad a Eternal Blue. [En línea]. Disponible en https://protegermipc.net/2017/07/03/utilidad-para-testear-la-vulnerabilidad-a-eternalblue

AMBOS KAI, 2015. Responsabilidad penal internacional en el ciberespacio, p. 13. Colombia: Universidad Externado de Colombia.

AREITIO Javier. 2008. Seguridad de la información: redes, informática y sistemas de información, p. 384. España: Paraninfo.

BACA, Daniel. 2016. Introducción a la Seguridad Informática. México: Grupo Editorial Patria. 12p.

BACA, Gabriel. 2016. Introducción a la seguridad informática, p. 218. México: Universidad Autónoma).

CARPENTIER Jean-Francois, 2016. La seguridad informática en la PYME: situación actual y mejores prácticas, p. 89. Barcelona: Ediciones ENI.

CARVAJAL Francisco, 2017. Gestión de servicios en el sistema informático, p. 88. Madrid: Editorial CEP.

CASAS, Eduardo. La red oscura: En las sombras de Internet: el cibermiedo y la persecución de los delitos tecnológicos. [En línea]. Madrid: La Esfera de los Libros. Disponible en https://books.google.com.co/books?id=GonFDQAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

CHICANO Esther, 2014. Gestión de servicios en el sistema informático. IFCT0509. Málaga: IC Editorial.

CHICANO Esther, 2014. MF0487_3: Auditoría de seguridad informática. Málaga: IC Editorial.

DEL PESO E. 2003. Manual de outsourcing informático. España: Ediciones Diaz de Santos.h76

Dirección General de Modernización Administrativa, Procedimiento e Impulso de la Administración Electrónica. MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

ECHEVERRÍA Guido, 2012. Procedimientos y medidas de seguridad informática, p.165.

EDITORIAL CEP, 2017. Cuerpo auxiliar (C2). Junta de comunidades de Castilla. La Mancha. Temario. p. 32. Madrid: Editorial CEP.

FERNÁNDEZ, Carlos, & PIATTINI, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. Madrid: AENOR, 2012.

FISHER, Royal. SEGURIDAD EN LO SISTEMAS INFORMATICOS. Madrid: Ediciones Díaz de Santos, S.A., 1988.

GARCÍA Héctor, 2006. Avances en informática y sistemas computacionales (CONAIS 2006), p. 122. México: Universidad Juárez Autónoma de Tabasco).
GÓMEZ Álvaro, 2017. Enciclopedia de la seguridad informática. 2° edición. España: Ra-Ma.

GÓMEZ, Luis, & ÁLVAREZ, Andrés. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid: AENOR, 2012.

GONZÁLEZ Juan José, De la Mata Norberto, Morón Esther… Adán Carmen, 2007. Delito e informática algunos aspectos, p.17. Bilbao: Universidad de DEUSTO.
GONZÁLEZ L. 2008. La sociedad de la información en Europa, p. 183. Madrid: Editorial REUS S.A.

MARCO María Jesús y Marco José María, 2010. Escaneando la informática, p.152. Barcelona: Editorial UOC.

MOLINER López Francisco Javier, 2005. Informáticos de la generalitat valenciana grupos A y B. bloque específico, temario volumen II, p. 203. España: Editorial MAD.
MOTYKA, Jakub. Esta herramienta te dice si tienes un PC vulnerable a Eternal Blue. [En línea]. Disponible en https://computerhoy.com/noticias/software/esta-herramienta-te-dice-si-tienes-pc-vulnerable-eternal-blue-64460

ORJUELA, Juan. Diseño de una arquitectura web distribuida de alta disponibilidad para sistemas de educación a distancia por medio de Oracle WebLogic Server. [En línea]. Juan Jose Orjuela Castillo. Disponible en https://books.google.com.co/books?id=eyq7BgAAQBAJ

PACHECO F. y Jara H. 2012. Hackers al descubierto: advierta sus vulnerabilidades evite que lo sorprendan, p.19. Argentina: USERS

PEQUEÑO M. 2015. MF0490_3. Gestión de servicio en sistema informático, p.380. España: Editorial ELEARLING S.L
Ramos Benjamín y Ribagorda Arturo, 2004. Avances en criptología y seguridad de la información, p. 353. Madrid: Diaz de Santos.

RASCAGNERES Paul. Seguridad Informática y Malwares. Barcelona: Ediciones ENI, 2016. 17p.

REVISTA DE LA SEGUNDA CORTE DEL DOCTORADO DE SEGURIDAD ESTRATÉGICA, 2014. Seguridad de la información, p. 31. Guatemala: Universidad San Carlos de Guatemala

SÁNCHEZ José Salvador, Chalmeta Ricardo, Óscar Coltell, Monfort Pilar y Campo Cristina.2003. ingeniería de proyectos informáticos: actividades y procedimientos, p.103. España: Universidad de Jaume

SOMMERVILLE Iam, 2005. Ingeniería del software, séptima edición, p.54. Madrid: PEARSON.

TÉLLEZ Julio, 1988. Contratos, riesgos y seguros informáticos, p. 33. México: Universidad Nacional Autónoma de México.

TERÁN David, 2014. Administración estratégica de la función informática. México: ALFAOMEGA

VALDIVIA Carlos, 2017. Informática industrial, p. 84. Madrid: Paraninfo.

VARIOS AUTORES, 2015. Seguridad informática Hacking ético, p. 201. Barcelona: Ediciones ENI.

VARIOS AUTORES, 2016. Técnicos especialistas en radiodiagnósticos: servicio andaluz de salud (SAS), p. 358. Madrid: Editorial CEP.

VARIOS AUTORES, 2017. Policía Nacional Escala Ejecutiva Inspector: volumen III, p. 54. Madrid: Editorial CEP.

VELASCO, Rubén. Comprueba si eres vulnerable al exploit EternalBlue con Eternal Blues. [En línea]. Disponible en https://www.softzone.es/2017/06/30/comprobar-vulnerabilidad-eternalblue

ZU, Jhonatan. ¿QUE ES EL PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB (OWASP)? [En línea]. Disponible en http://seguridadaguijon.blogspot.com/2018/03/que-es-owasp.html

RAE

RESUMEN ANALITICO ESPECIALIZADO - RAE
1. TEMA
Infraestructura tecnológica y seguridad en redes
2. TITULO
Diseño del plan estratégico de seguridad de la información (PESI) para una entidad hipotética; según vulnerabilidades identificadas en ambientes de pruebas controlados
3. AUTORES
Carlos Alberto Díaz Carmona Luis Manuel Herrera López
4. FUENTE BIBLIOGRAFICA
Se consultaron 54 fuentes bibliográficas para el desarrollo de las diferentes partes del proyecto, donde la más relevante fue: Título: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. [electrónico]. Madrid, octubre de 2012. [Consultado: 28 de abril de 2019]. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
5. AÑO
2020
6. RESUMEN
El servidor web de una entidad hipotética ha sido víctima de ataques Defacement y Eternal Blue por parte de Black Hackers, en las sedes ubicadas en las ciudades de Bogotá y Cali respectivamente. Dado esto y al proceso de expansión que inician en el presente año, la alta dirección ha decidido contratar a un experto en seguridad informática con el fin de realizar las pruebas de vulnerabilidad que ayuden a descifrar el método de intrusión utilizado, y cada uno de los pasos que siguieron para lograrlo. Para ello se utilizarán herramientas de análisis de seguridad como los Nmap, Metasploit y OpenVas encontradas en la distribución Kali Linux. Al final del análisis se entregará un informe detallado del procedimiento llevado a cabo y de un Plan Estratégico de Seguridad de la Información a implementar en la organización con el fin de solventar los problemas de seguridad en los sistemas de información y prevenir problemas futuros, con el fin de garantizar la seguridad en la prestación de los servicios a sus clientes.
7. PALABRAS CLAVES
Vulnerabilidad, riesgos, seguridad, Plan Estratégico, amenazas, normativas, ataques, ambiente de pruebas, PESI.
8. CONTENIDO

Este proyecto se basa en una empresa hipotética la cual presenta problemas de seguridad en sus sistemas de información. Para dar solución, se realiza la contratación de personal capacitado los cuales se encargarán de dictaminar las posibles causas de lo ocurrido. Como primera medida se realiza un análisis de vulnerabilidades recreando la situación presentada sobre un ambiente controlado y con la ayuda de herramientas de software obtener las conclusiones que permitan realizar las correcciones que se consideren pertinentes.
Posteriormente se realiza el análisis de la gestión de riesgos basado en la metodología Magerit para posteriormente diseñar el plan estratégico de seguridad de la información PESI, en donde se incluyen los proyectos de seguridad de la información que permitan reducir al máximo posible el riesgo de que se vuelvan a presentar situaciones similares.

9. DESCRICION DEL PROBLEMA DE INVESTIGACIÓN

Una organización hipotética ha sido víctima de ataques informáticos por parte de *black hackers*, los cuales utilizaron ataques de *Defacement* y Eternal Blue. Estos ataques afectaron el funcionamiento del servidor web de la ciudad de Bogotá y el servidor de la ciudad de Cali, viéndose comprometida la confidencialidad de las contraseñas y de la información de los usuarios almacenada en la base de datos. Adicionalmente, dado al proceso de expansión que inicia este año, la alta dirección se encuentra preocupada por la seguridad de la información y de los sistemas que maneja la organización y teme que no se entregue un servicio de calidad a sus clientes.

10. OBJETIVO GENERAL

Diseñar un plan estratégico de Seguridad de la Información en una organización que permita la aplicación de controles y políticas que garanticen la corrección de vulnerabilidades detectadas a través de diferentes herramientas de seguridad y prevención de diferentes ataques como *Defacement* y *Eternal Blue*.

11. OBJETIVOS ESPECIFICOS

• Configurar un ambiente de pruebas para el análisis de vulnerabilidad y ejecución de ataques *Defacement* y Eternal Blue

• Ejecutar los ataques *Defacement* y Eternal Blue en un ambiente controlado de pruebas.

• Realizar el análisis de gestión de riesgos como parte del plan estratégico de Seguridad de la Información.

• Sugerir a partir de los objetivos de la organización, el diseño de un Plan Estratégico de la Seguridad de la Información basado en metodologías de la gestión de riesgos informáticos.

12. METODOLOGIA

Para la realización del primer ataque, *Defacement*, se realiza la instalación y configuración de una máquina virtual en VirtualBox con sistema operativo Metasploitable 2, el cual simulará ser el sistema atacado de la registraduría. Esta máquina virtual se configura en una red NAT.

Posteriormente, se realiza la instalación y configuración de una máquina virtual en VirtualBox con el sistema operativo Kali Linux, desde la cual se lleva a cabo el ataque al sistema Metasploitable 2. Esta máquina virtual se configura en una red NAT. Durante la preparación del entorno, primero se realiza la actualización de Kali Linux.

Para escanear las vulnerabilidades del sistema Metasploitable, se utilizan las herramientas Nmap que viene instalada en el sistema operativo Kali Linux y OpenVas, la cual se debe instalar para realizar el escaneo.

Una de las vulnerabilidades en el sistema Metasploitable, es a un ataque cgi. Se utiliza el *Metasploit* Framework para encontrar y utilizar un *exploit* que permita materializar la vulnerabilidad encontrada.

Para realizar el segundo ataque, Eternal Blue, se realiza la instalación sobre una máquina virtual en el programa Virtual Box del sistema operativo Windows 7, este no cuenta con las ultimas actualizaciones lo cual es un caso muy común, además de que el firewall no cuenta con la configuración correcta. Esta máquina también se configura en una red NAT.

Se realiza un escaneo de las vulnerabilidades del sistema con Windows 7 y posteriormente se procede a utilizar el *Metasploit Framework* para encontrar y utilizar un *exploit* que permita explotar la vulnerabilidad en el servicio SMB.

Durante la realización de cada una de las actividades anteriores, se realizan consultas en internet para conocer los comandos a utilizar. Adicionalmente, Durante el desarrollo de los análisis se registrará el paso a paso de los procedimientos realizados con registros de capturas de pantalla utilizando los lineamientos establecidos por la norma NTC 1486.

El tipo de investigación a utilizar es aplicado, dado que se busca dar respuesta a interrogantes puntuales acerca de un problema conocido. Las técnicas de recolección de datos que se utilizarán en el proyecto son la observación y entrevistas.

13. PRINCIPALES REFERENTES TEÓRICOS Y CONCEPTUALES

Se realizó la consulta de varias referencias teóricas y conceptuales, y se enfoca en el análisis de las vulnerabilidades, realización de los ataques, análisis de riesgos de acuerdo con la metodología MAGERIT.

14. RESULTADOS

Cómo resultado de la implementación del proyecto se elaboraron los siguientes productos y/o entregables:

- Máquinas Virtuales con ambientes de Prueba.
- Análisis de riesgos.
- Plan de Tratamiento de riesgos.
- Plan Estratégico de la Seguridad de la Información.

15. CONCLUSIONES

A partir de la recreación de las configuraciones y topología de red pertenecientes a la empresa hipotética en su sede en Bogotá y evidenciar las vulnerabilidades que albergaban los sistemas de información, se puede concluir a partir de los hallazgos, la importancia de la seguridad informática, y como con la realización de buenas prácticas se pueden disminuir los riesgos ante amenazas cibernéticas.

Es importante tener siempre presente la información como activo fundamental de todas las compañías, por ello al momento de pensar en la implementación de sistemas de seguridad, se debe realizar un análisis previo de gestión de riesgo, alineado con el plan estratégico de la seguridad que permita identificar cuáles son los riesgos asociados a los sistemas de información de la organización y como mitigarlos.

Así mismo, para lograr el éxito en la implementación de un plan de gestión de seguridad informática, es necesario apoyarse en estándares internacionales como guía, que ayuden con la elaboración de un plan de acción, al igual que en metodologías como Magerit las cuales ayudan a comprender como mitigar un riesgo a partir de la posibilidad de que este suceda.