PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA TALLER INDUSTRIAL ALKAN S.A.S DE LA CIUDAD GUADALAJARA DE BUGA, VALLE PARA IDENTIFICAR VULNERABILIDADES

JAVIER MARMOLEJO SERRANO

ADRIAN PASTRANA FRANCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI

Escuela: CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

Programa: ESPECIALIZACION EN SEGURIDAD INFORMATICA

2018

PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA TALLER INDUSTRIAL ALKAN S.A.S DE LA CIUDAD GUADALAJARA DE BUGA, VALLE PARA IDENTIFICAR VULNERABILIDADES

JAVIER MARMOLEJO SERRANO

ADRIAN PASTRANA FRANCO

Proyecto para optar por el título de Especialista en Seguridad Informática

Asesor Temático

Ingeniero Juan José Cruz

Directora de proyecto

MG. Yina Alexandra González Sanabria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN - VIACI

Escuela: CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

Programa: ESPECIALIZACION EN SEGURIDAD INFORMATICA

2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Palmira, 27 de Mayo de 2018

DEDICATORIA

Este trabajo está dedicado a nuestras familias, por cuanto todo su apoyo en la formación académica fue esencial para sacar adelante nuestros sueños para un futuro mejor. A nuestros amigos, y a Dios por darnos la posibilidad de llegar a esta meta.

CONTENIDO

LISTA DE TABLAS

Lista de ilustraciones

AGRADECIMIENTOS

Agradecemos a los profesores de la Universidad Nacional Abierta y a Distancia UNAD, quienes fueron guía y apoyo para el desarrollo personal y en la formación académica adquirida a lo largo de este proyecto.

A nuestras familias, por enseñarnos la importancia de la perseverancia en la consecución de nuestros objetivos.

A la Mg. Yina Alexandra González Sanabria, directora del presente desarrollo quien con su apoyo, guio para direccionar y culminar el trabajo en el que se representa toda nuestra formación.

A la empresa taller industrial Alkan, por permitirnos poner en pie este proyecto en su organización.

En general a todos los que se vieron involucrados con este trabajo, les agradecemos profundamente por su apoyo y compromiso.

GLOSARIO

PENTESTING: Las pruebas de penetración (también llamadas “pen-testing”) son una práctica para poner a prueba un sistema informático, red o aplicación web para identificar vulnerabilidades que un atacante podría explotar.

VULNERABILIDAD: Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.

RIESGO: El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

AMENAZA: Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.[1]

KALILINUX: Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni and Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a

[1] SANTANA, Carlos. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En línea}. 2012. {7 Septiembre de 2012}. Disponible en https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.[2]

WIRESHARK: Es una herramienta multiplataforma con interfaz gráfica para el análisis de red, producto de la evolución de Ethereal. Incluye la herramienta Tshark en modo consola para capturas, análisis de red, entre otras posibilidades. Al usar las librerias pcap, su uso es similar a Tcpdump y Windump. Este permite ver, a un nivel bajo y detallado, consultar todo lo que está ocurriendo en la red.[3]

NMAP: ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.[4]

MAGERIT: es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

---

[2] EcuRed. Kali Linux. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://www.ecured.cu/Kali_linux
[3] EcuRed. Op. Cit.
[4] EcuRed. Op. Cit.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.[5]

HACKERS: persona o una comunidad que posee conocimientos en el área de informática y se dedica a acceder en los sistemas informáticos para realizar modificaciones en el mismo. Los hackers también son conocidos como “piratas informáticos”.[6]

[5] Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

[6] FRANCO, Tovar. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. {En línea}. 2017. {5 Diciembre de 2017}. Disponible en http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

INTRODUCCIÓN

La información es el activo más importante de las entidades públicas, privadas, o de cualquier otra naturaleza, para lo cual las personas encargadas de la seguridad de los sistemas informáticos deben establecer procedimientos y herramientas eficientes para el envío de datos de una forma segura. La seguridad de la información es una responsabilidad y compromiso de gran importancia, razón por la cual se debe adoptar los mecanismos esenciales para la protección de la información y no estar expuesta a ataques informáticos, y la proyección de la seguridad en una entidad debe crear certidumbre y viabilidad. La insensibilidad en los controles y uso inadecuado de la información en las organizaciones ocasiona que tengan mayor probabilidad a ser vulnerados sus sistemas. Los delincuentes informáticos no solo atacan grandes entidades, regularmente son atacadas pequeñas empresas por personal interno que las constituyen. Para lograr la mitigación de los riesgos de seguridad presentes en una organización es necesario la ejecución de pruebas de testeo a la red de datos y lograr diagnosticar las vulnerabilidades existentes en los sistemas de información, efectuando la evaluación de las mismas y el planteamiento de estrategias de mitigación de los riesgos hallados para la prevención y mejora de la seguridad en el control de acceso fundamentado en los estándares actuales de la norma técnica colombiana NTC-ISO/IEC 27001, y estos estándares son aplicados con pruebas de penetración a la infraestructura tecnológica de la empresa taller industrial Alkan S.A de la ciudad Guadalajara de Buga, valle para identificar vulnerabilidades, esta entidad ha venido funcionando de manera estable en el mercado durante los últimos años; demostrando un evidente crecimiento en la información registrada en su base de datos, y en el préstamo de sus servicios, por tanto quiere garantizar un óptimo cubrimiento al acceso de su red a través de un sistema seguro que los proteja de cualquier ataque informático que se presente.

1 DEFINICION DEL PROBLEMA

PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA TALLER INDUSTRIAL ALKAN S.A.S DE LA CIUDAD GUADALAJARA BUGA, VALLE PARA IDENTIFICAR VULNERABILIDADES

1.1 ANTECEDENTES DEL PROBLEMA

La empresa taller industrial Alkan nace en la ciudad Guadalajara de Buga hace 48 años, está dedicada a la ejecución de trabajos relacionados con el área metalmecánica, ingeniería, tratamientos anticorrosivos, recubrimientos, aislamientos, mantenimiento mecánico, eléctrico y afines orientado a satisfacer las necesidades y expectativas de sus clientes, cumpliendo con las especificaciones y los acuerdos contractuales establecidos.

En el mundo de hoy, la información es un recurso que como el resto de los activos, tiene un gran valor para la empresa, este debe ser debidamente protegido, asegurando la continuidad de los servicios que se prestan por el servidor de la información, reduciendo los riesgos y ayudando a una mejor ejecución en sus procesos que propenden a mejorar la calidad del servicio en la atención a sus clientes. En el servidor de gestión de la información de la empresa, se maneja información, comercial, reportes, correo interno y externo, los cuales no pueden ser arriesgados a un ataque informático, la seguridad de la información como la confidencialidad, integridad y disponibilidad oportuna. El taller industrial Alkan no ha implementado estrategias de reducción de riesgos en el sistema de la seguridad de la Información, para realizar análisis, control y optimización demandadas por la ISO/IEC 27001[7] en la cual se especifica “los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la

[7] Norma Iso 27001 (2017). - Sistema de Gestión de la Seguridad de la Información. Disponible en http://www.gesconsultor.com/iso-27001.html

Seguridad de la Información (SGSI), definición del alcance del SGSI, definición de una Política de Seguridad", debido a que en sus inicios era una empresa muy pequeña y no se pensó que esta crecería de una manera acelerada y llegar a tener tantos clientes, para lo cual no puede mitigar los riesgos en la seguridad informática.

Hay muchos tipos de amenazas los cuales ponen en peligro los servicios prestados por el sistema de información, generando daños en los procesos administrativos y comerciales de la empresa, como ha sucedido en varias empresas de servicio tal como lo especifica el ministro de Defensa, Luis Carlos Villegas, quien dijo que las autoridades atendieron entre enero y agosto del 2.017, 5.500 ataques cibernéticos, que han afectado principalmente al sector privado[8], Actualmente la empresa presenta algunas dificultades en la seguridad de la información a partir de su segundo año de funcionamiento, cuando se detectó la desaparición de alguna información sobre datos de clientes, bloqueo de archivos, perdidas de conectividad sin explicación alguna, duplicación de la información y derivación de información comercial no propia de la empresa por parte externa.

1.2 PLANTEAMIENTO DEL PROBLEMA

Surge de la necesidad de mantener control frente los riesgos que puede correr los sistemas operativos y la base de datos en la empresa taller Alkan S.A.S

Luego de hallar esto se propone analizar por medio de herramientas de pentesting con el objetivo de solucionar las vulnerabilidades o ataques de los hackers.

[8] El colombiano.com (2017). Hackers han realizado 5.500 ataques cibernéticos en 2017. Disponible en http://www.elcolombiano.com/colombia/hackers-han-realizado-5-500-ataques-ciberneticos-en-2017-YD7126742

Al aplicar un reconocimiento de vulnerabilidades al sistema de gestión de seguridad de la información con ayuda de herramientas como laboratorios de pruebas de penetración con diversas herramientas según Franco, Tovar (2013)[9], las cuales permiten evaluar las condiciones de seguridad ayudando a plantear un plan de reducción de vulnerabilidades que a futuro mantenga un sistema de información confiable, íntegro y disponible, evitando riesgos a los cuales estaría comprometido.

1.3 FORMULACIÓN DEL PROBLEMA

¿Las pruebas de penetración a la red de la empresa solucionarían los problemas de vulnerabilidad en la seguridad de la información de la empresa taller Industrial Alkan S.A.S?

[9] Franco, Tovar (2017). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Disponible en http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar pruebas de penetración a la infraestructura tecnológica de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle para identificar vulnerabilidades.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento de los activos de información de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle mediante la metodología Magerit.

- Aplicar pruebas de penetración a la red de datos empleando la metodología del ethical hacking con la herramienta Kali Linux para diagnosticar las vulnerabilidades de seguridad de la información de la empresa Talleres Alkan de la ciudad Guadalajara de Buga, Valle.

- Valorar las vulnerabilidades encontradas según los riesgos detectados en las pruebas de testeo de red y su efecto en el sistema de información.

- Plantear estrategias de reducción de los riesgos encontrados para evitar y reforzar la seguridad de la información.

3 JUSTIFICACIÓN

La empresa taller Industrial Alkan S.A es una empresa con buena trayectoria, con un excelente crecimiento debido a factores de los excelentes servicios que ofrecen en el área metalmecánica, así como las excelentes estrategias de servicio de alto standing. Para su funcionamiento se hace uso de las redes sociales que han gozado de excelente aceptación y por lo tanto se hace indispensable tener una buena protección en la seguridad informática que permita salvaguardar la comunicación e información. Hasta la fecha esta empresa no cuenta con la seguridad informática adecuada y ha presentado problemas como la desaparición de alguna información sobre datos de clientes, bloqueo de archivos, perdidas de conectividad sin explicación alguna, duplicación de la información y derivación de información comercial no propia de la empresa por parte externa.

El sistema de gestión de la seguridad en la información está orientado en proteger el sistema de información utilizando protocolos, normas y herramientas para disminuir daños en el software, bases de datos y toda la información empresarial. En el caso de la empresa se beneficiarían de este proyecto en cuanto la conservación de la integridad, disponibilidad, confidencialidad, autenticidad de la información, en el desarrollo y crecimiento de sus metas, para asegurar los sistemas informáticos y evitar pérdidas de información lo cual influye en el cumplimiento de la misión empresarial, de igual manera este beneficio causara un impacto positivo en el sector de servicios metalmecánicos que es uno de los campos económicos a explotar en la región del Valle del Cauca.

La importancia de la seguridad informática

De acuerdo a la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001[10], las instituciones públicas y empresas privadas se ven obligadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas. Debido a esto es primordial que el sistema de la información de la empresa taller industrial Alkan S.A que contiene información comercial, reportes, correspondencia interna y externa, sea un sistema vital y seguro para la empresa la cual se obliga a estar protegida.

Al efectuar un rastreo de vulnerabilidades al sistema de la información, permitirá evaluar sus condiciones de seguridad lo cual facilitara el planteamiento de un plan de reducción de vulnerabilidades que a futuro mantenga un sistema de información confiable, íntegro y disponible que además evitará los riesgos a los cuales estaría comprometido reduciendo el impacto negativo en el funcionamiento de la empresa.

Recomendaciones de la OCDE[11]

Establecer nuevas políticas prácticas, medidas y procedimientos, o modificar los existentes, para reflejar y tomar en consideración el contenido de las Directrices para la Seguridad de Sistemas y Redes de la información, mediante la adopción y promoción de una cultura de seguridad, tal y como se establece en dichas

[10] ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf
[11] OCDE.Organización para la Cooperación y Desarrollo Económico. Disponible en http://www.oecd.org/internet/ieconomy/34912912.pdf

Directrices; Desarrollar esfuerzos para consultar, coordinar y cooperar a nivel nacional e internacional, a los efectos de poder implantar estas Directrices.

Recomendaciones ministerio de las tecnologías de la información y telecomunicación (MINTIC)[12]

Las recomendaciones que hace el ministerio de las tecnologías de la información y telecomunicación a las empresas se relacionan en el siguiente listado:

• Actualice y licencie sus cortafuegos y antivirus.

• Realice revisión periódica de su listado de contactos y practique la utilización de firma digital o autenticación del mensaje a través de hash.

• No realice transacciones desde páginas web no confiables

• No instale herramientas de escritorio remoto, siempre y cuando no se almacene un llavero de claves seguro y confiable.

• Evite conectarse desde redes inalámbricas abiertas que no tienen ninguna seguridad.

• Cerciórese de la información de contacto con el fin de verificar el auténtico originador del mensaje.

• No descomprima archivos de extensión desconocida sin antes verificar el “vista previa” el contenido del mismo.

• Elimine correos electrónicos “Spam”, de esta forma evitará ir a sitios web no seguros.

• Actualice los parches de seguridad del navegador web.

[12] MINTIC. (06 de Noviembre de 2016). Guía para la Implementación de. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

• Gestión adecuada de información confidencial y de terceros (títulos financieros, chequeras, tarjetas, productos crediticios, etc.)

• Implemente servidor de correos electrónicos SPF (Sender Policy Framework).

ISO 27001 (2.006)[13]

La dirección debe revisar el SGSI de la organización a intervalos planificados (por lo menos una vez al año), para asegurar su conveniencia, suficiencia y eficacia continuas. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros

Las entradas para la revisión por la dirección deben incluir:

a) Resultados de las auditorías y revisiones del SGSI.
b) Retroalimentación de las partes interesadas.
c) Técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del SGSI.
d) Estado de las acciones correctivas y preventivas.
e) Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
f) Resultados de las mediciones de eficacia.
g) Acciones de seguimiento resultantes de revisiones anteriores por la dirección;
h) Cualquier cambio que pueda afectar el SGSI.
i) Recomendaciones para mejoras.

[13] NTC-ISO/IEC-27001. (22 de Marzo de 2006). TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). Obtenido de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20

4 MARCO DE REFERENCIA

4.1 MARCO CONTEXTUAL

4.1.1 Nombre de la Empresa

Taller industrial Alkan S.A.S

4.1.2 Misión

Realizar todas aquellas actividades dirigidas a cubrir todos los requerimientos de las empresas la cual se enfoca al mantenimiento reparación y fabricación de piezas, maquinado de repuestos y accesorios de máquinas equipos para diferentes sectores industriales orientando nuestro trabajo hacia la satisfacción entera de nuestros clientes, con la mejor calidad y el mejor servicio, encaminados siempre hacia la calidad total.

4.1.3 Visión

La empresa tiene como visión consolidarse líder en la prestación del servicio al sector metalmecánico, reconocidos como una organización seria, orientado hacia el trabajo coordinado por el cumplimiento de objetivos y metas logrando así la satisfacción y buen desempeño en la consecución las necesidades de nuestros clientes, ofreciendo el mejor servicio en el mercado.[14]

[14] Informa (2018). Directorio de empresas de Colombia. Disponible en https://www.informacion-empresas.co/Empresa_TALLER-INDUSTRIAL-ALKAN-SAS.html

4.1.4 Organización

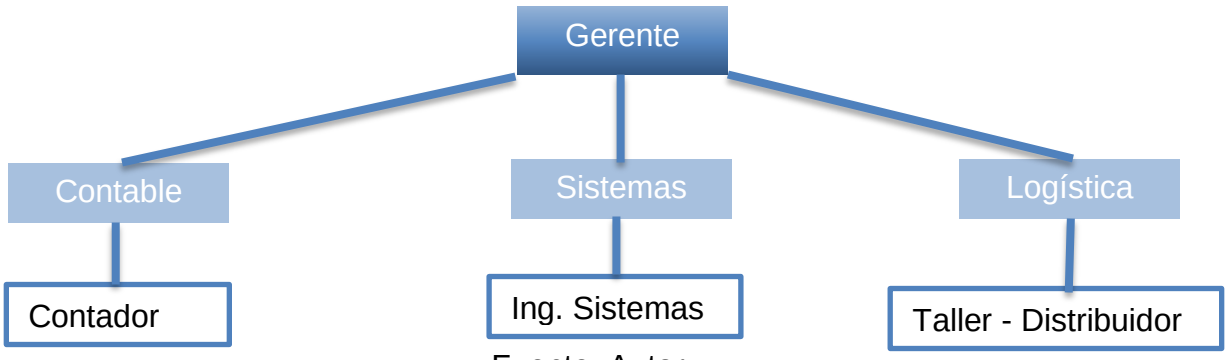
Taller industrial Alkan S.A., es una empresa del sector industrial, especializado en prestar servicios a empresas con necesidades en el área metalmecánica satisfaciendo por completo sus requerimientos.

Se conoce a fondo las necesidades de las empresas dedicadas al sector industrial y se ha fortalecido en los por menores que marcan la diferencia en los servicios convencionalmente ofrecidos en el mercado como lo son:

- Entregas en un menor tiempo, ya que esto repercute directamente en la producción eficaz de los clientes, los cuales tienen este como su principal fuente de ingresos.
- Se cuenta con cobertura a nivel Departamental.

Haciendo que el objetivo principal sea la satisfacción de las necesidades de los clientes, garantizando la simpleza y transparencia del servicio, en un mercado industrial de responsabilidad y respeto hacia los clientes y colaboradores.

Ilustración 1. Organigrama Taller Industrial Alkan S.A.S.



Fuente. Autor

4.2 MARCO TEORICO

En la línea del tiempo de la seguridad informática se observa un gran crecimiento cada día, en la década de los noventa la seguridad informática se centraba en proteger simplemente que el usuario no dañara el sistema operativo y como máxima protección se colocaba un antivirus para que no dañara la información.

Con la aparición de la internet, la seguridad informática se fue centrando en el sistema redes, procurando proteger servidores, equipos y controlando la seguridad a través de firewall, lo cual generaba nuevas posibilidades de aparición de vulnerabilidades que podrían ser explotadas por aquellas personas que sabían que hacer para obtener información y qué hacer con ella. El perfil de los atacantes antes se centraba en acceder a un sitio donde nadie más podía llegar o simplemente infectar un sistema con un virus pero todo sin ánimo de lucro, en la actualidad, los atacantes les importa la información, pero la mayoría de estos lo hacen como un reto, se aprovechan de las vulnerabilidades en los sistemas y las redes para acceder a la información sensible de una entidad con ánimo de lucro, ante esta situación las entidades se protegen con nuevas tecnología que están desarrolladas en software para repeler estas debilidades del sistema. El premio que buscan los atacantes es apoderarse de las bases de datos que es una especie de almacén el cual consiste en guardar información de forma ordenada permitiendo buscar y utilizar fácilmente, actualmente existen numerosas bases de datos dependiendo de la necesidad de los usuarios. Se debe tener en cuenta el concepto de seguridad informática en todo este tema, el cual está compuesto en tres pilares fundamentales, los cuales se deben cumplir en cualquier sistema informático: La confidencialidad; este pilar hace referencia a la privacidad de la información, la integridad es decir que la información sea correcta y no haber sido modificada, y la disponibilidad que hace referencia a aquella información a la que

se puede acceder cuando se necesite[15], con la aplicación de la seguridad informática se debe obtener la protección del sistema de acceso a la información por parte de personal o programas no autorizados. Para tener bases sólidas y controlar, repeler estas debilidades de los sistemas, se debe conocer los siguientes conceptos:

Metodología ethical hacking

Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades, haciendo uso de las herramientas que ofrece el sistema operativo de Pentesting Kali Linux como Nmap, Metasploit, Wireshark, Owasp zap, Armitage, Suite aircrack-ng entre otras para que los administradores de TI y personas en general tomen medidas preventivas contra ataques informáticos. Linux Adictos, (2017)[16].

Vulnerabilidad

Una vulnerabilidad es una debilidad en algún recurso informático que se aprovecha para ser accedida de forma intencional o accidentalmente, estas pueden provenir de muchas fuentes como el diseño, implementación de los sistemas, los procedimientos de seguridad y controles internos, descuido de los usuarios; protecciones inadecuadas o insuficientes de forma físicas y lógicas,

[15] FIRMA-E consultoría & desarrollo, Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad, Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[16] Linux adictos (2017). Herramientas de Kali Linux. Disponible en https://www.linuxadictos.com/las-5-mejores-herramientas-encontraremos-kali-linux.html

procedimentales o legales de alguno de los recursos informáticos. Estas al ser accedidas resultan en fisuras en la seguridad con impactos perjudicial para la organización. Voutssás Márquez, 2010[17].

También la vulnerabilidad (en términos de informática) es un fallo en un sistema de información que coloca en riesgo la seguridad de la información permitiendo que los atacantes puedan involucrar la integridad, disponibilidad o confidencialidad del sistema de información, por lo que es necesario eliminarlas en corto tiempo. Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas. INCIBE, 2017[18].

Control de acceso

El Control de Acceso a la red es aplicado para "controlar el acceso de los usuarios a la red, verificar que todos los dispositivos que se conectan a las redes de una organización cumplan las políticas de seguridad establecidas para prevenir amenazas como la entrada de virus, salida de información, etc." GUERRERO ERAZO, LASSO GARCES, & LEGARDA MUÑOZ, 2015[19].

[17] Voutssás Márquez,J.Preservación documental digital y seguridad informática. Investigación bibliotecológica, 127-155.
[18] INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[19] GUERRERO ERAZO, H. A., LASSO GARCES, L. A., & LEGARDA MUÑOZ, P. A. UNAD. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3451/1/5203676.pdf

Seguridad informática

La seguridad informática es la encargada de proyectar los modelos, los procedimientos, métodos y técnicas para adquirir un sistema de información genuino y seguro. Protege contra posibles riesgos, amenazas, vulnerabilidades originados por la incorrecta utilización de tecnologías de información. Las entidades públicas y privadas deben establecer políticas de seguridad implementando mecanismos de protección y evitar los medios de acceso que generen vulnerabilidad al sistema de la información. Sus objetivos son:

- Conservar la integridad, disponibilidad, confidencialidad, autenticidad y no repudio de la información.
- Preservar los activos informáticos de la empresa, como la infraestructura tecnológica (hardware, software), mediante el uso de estrategias apropiadas, la seguridad informática apoya a la empresa en el desarrollo de las metas, protegiendo los bienes materiales e inmateriales.
- Proteger los sistemas informáticos para impedir grandes pérdidas de información lo cual influye en el cumplimiento la misión empresarial.
- Los directivos de las empresas deberían agregar a los objetivos empresariales la seguridad informática como una herramienta para controlar y mitigar los riesgos.
- Se entiende por seguridad informática la característica de cualquier sistema informático, que hace que esté libre de todo peligro, daño o riesgo. Como no hay sistema infalible, se trata de que el sistema sea lo más fiable posible. Purificación, 2.010[20.]

[20] AGUILERA, Purificación. Seguridad informática. Editex, 2010. p.9

Sistema de Gestión de información

Encargado de seleccionar, procesar y distribuir la información procedente de las partes internas, externas y corporativas:

- Información interna. La producida en la actividad cotidiana de la institución
- Información externa. La adquirida por la institución para disponer de información sobre los temas de su interés
- Información corporativa o pública. La que la institución emite al exterior

Las funciones de la Gestión Información abarcarían:

1) Determinar las necesidades de información en correspondencia a sus funciones y actividades
2) Mejora de los canales de comunicación y acceso a la información
3) Mejora de los procesos informativos
4) Empleo eficiente de los recursos Arévalo, 2012[21.]

Un sistema de información está integrado por un conjunto de componentes que almacenan, procesan y distribuyen información. Cuando mencionamos la gestión de información nos referimos a la gestión que se desarrolla en un sistema de información (si se trata de que el sistema tenga como propósito obtener salidas informacionales). Puede tratarse, en función de lo antes explicado, del subsistema de información de una organización. PONJUÁN DANTE, 2007[22.]

[21] Arévalo, J. A. (2012). MediCiego. Disponible en http://www.bvs.sld.cu/revistas/mciego/alfin_2012/alfin_folder/2012%20Unidad%206/Bibliograf%EDa/Lect%20B%E1sicas/Lectura_basica_5.Gestion_de_la_informacion_gestion_de_contenidos_y_conocimiento.pdf

[22] PONJUÁN DANTE, G. (2007). Gestión de información. Dimensiones e implementación para el éxito organizacional. La Habana - Cuba: TREA.

4.3 MARCO CONCEPTUAL

Para el desarrollo de este trabajo se utiliza el Pentesting, que según Jorge Luis Ramos Ramos[23], es la práctica de atacar diversos entornos con la intención de descubrir amenazas, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques internos o externos hacia esos equipos o sistemas, siendo el más indicado para la aplicación de este proyecto.

Ahora bien, se hace necesario definir el concepto de amenaza, que para el Departamento de Seguridad Informática de la Universidad Nacional de Luján[24] es todo elemento o acción capaz de atentar contra la seguridad de la información, esta definición sirve para identificar y caracterizar todas aquellas amenazas a las que está expuesta la información del Taller Industrial Alkan.

También es indispensable definir el concepto de confidencialidad, que para Voutssás[25] quiere decir que la información debe estar disponible siempre, pero sólo para las personas autorizadas, durante las circunstancias y bajo condiciones válidas y preestablecidas, y para el Taller Industrial Alkan es importante implementar políticas de confidencialidad para verificar el acceso a la información únicamente por los empleados encargados de cada área específica.

Continuando con el siguiente pilar de la seguridad informática, se encuentra que la información debe tener integridad para que la información sea exacta y completa, no dando lugar a modificaciones de cualquier tipo, está la define Voutssás [26]como la confianza de un documento de archivo como tal; esto es, la cualidad de un documento de archivo de ser lo que pretende ser sin alteraciones o corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo.

---

[23] RAMOS RAMOS Jorge Luis, PRUEBAS DE PENETRACIÓN O PENT TEST, Op Cit.

[24] UNIVERSIDAD NACIONAL DE LUJAN, Amenazas a la Seguridad de la Información, Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[25] VOUTSSÁS MÁRQUEZ, Juan. Preservación documental digital y seguridad informática, Op. Cit.

[26] VOUTSSÁS MÁRQUEZ, Juan. Preservación documental digital y seguridad informática, Op. Cit.

Continuando con el ultimo pilar de la seguridad informática, la disponibilidad que el mismo Voutssás la define como la facilidad de poder acceder a la información cuando, como sea y por quien sea necesario, esto es indispensable si lo que se quiere en el Taller Industrial Alkan es asegurar la información para que sea visible solo para el personal autorizado.

Teniendo en cuenta los conceptos anteriores se hace indispensable analizar la problemática actual de la producción y acumulación de información en forma de documentos electrónicos o digitales, así como los problemas derivados del acceso a esa información, sobre todo en red, dado que esto podría implicar riesgo y pérdida de esa información. Se determinan los riesgos, amenazas vulnerabilidades, etcétera, que afectan a esa información, así como diversas estrategias para establecer la seguridad informática y la relación de ésta con la preservación confiable de esa información. Se estudian y establecen con detalle los factores que inciden a favor y en contra de los documentos digitales, siendo el riesgo una posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información[27].

4.3.1 ANTECEDENTES / ESTADO DEL ARTE

Como antecedentes del proyecto se realiza una búsqueda encontrando el trabajo Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios, de David A. Franco, Jorge L. Perea y Luis C. Tovar (2013)[28] pertenecientes a la Universidad de Cartagena, donde el objetivo principal de este trabajo fue diseñar un nuevo enfoque para la detección y evaluación de vulnerabilidades en equipos de red mediante la técnica de identificación de servicios. Este enfoque consiste en determinar los nombres y versiones de los

[27] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 op, cit,

[28] FRANCO David, PEREA Jorge, y TOVAR Luis (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

servicios activos en un equipo de red para luego buscar las vulnerabilidades de seguridad de los mismos en la Base de Datos Nacional de Vulnerabilidades. Se desarrolló una herramienta computacional llamada UdeCEscaner y se escogieron varios laboratorios de pruebas. Los resultados permitieron determinar que el enfoque propuesto es efectivo para la identificación y evaluación de vulnerabilidades. Se concluye que la implementación del enfoque propuesto ayuda a los administradores de las tecnologías de la información y la comunicación en la mejor comprensión de los riesgos reales a los que están expuestos, facilitando la mitigación de vulnerabilidades de seguridad.

Otro trabajo que sirvió de referente es el Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia) [29]de Julián Alberto Monsalve Pulido, Fredy Andrés Aponte Novoa y David Fernando Chaves Tamayo en el cual se expone el resultado del diagnóstico de seguridad informática realizado a una organización privada en el departamento de Boyacá (Colombia), y de la creación y aplicación de un plan de gestión de vulnerabilidades diseñado a la medida de las necesidades de dicha organización. Se inició la investigación con el levantamiento del inventario tecnológico de la empresa, para identificar los problemas que pueden causar alguna vulnerabilidad que afecte la seguridad de la información. Tras una etapa de 6 meses de monitoreo del plan de gestión dentro de la empresa, se evidenció la efectividad de éste, pues se logró una reducción del 70% en las vulnerabilidades, con la aplicación de algunos remedios previamente diseñados. Por otro lado, en el artículo se muestran algunos cuadros comparativos de herramientas informáticas que fueron seleccionadas y utilizadas en la aplicación de las etapas del plan de gestión, ya que pueden ayudar a investigaciones futuras a la selección de herramientas para el monitoreo y gestión de vulnerabilidades.

[29] MONSALVE Julián, APONTE Fredy y CHAVES David. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia), En: Revista Facultad de Ingeniería (Fac. Ing.), Vol. 23, No. 37 (Jul-Dic, 2014); pp. 65-72.

Continuando con la búsqueda de información para la realización de este proyecto, se encuentra el aporte del mexicano Juan Voutssas M. con su proyecto Preservación documental digital y seguridad informática[30] donde expone un análisis de la problemática actual que existe con la producción y acumulación mundial de información en forma de documentos electrónicos o digitales, así como los problemas derivados del acceso de esa información, sobre todo en red, dado que esto podría implicar riesgo y pérdida de esa información. Se determinan los riesgos, amenazas vulnerabilidades, etcétera, que afectan a esa información, así como diversas estrategias para establecer la seguridad informática y la relación de ésta con la preservación confiable de esa información. Se estudian y establecen con detalle los factores que inciden a favor y en contra de los documentos digitales.

En esta investigación, como dice Jorge Luis Ramos Ramos de la Universidad Mayor de San Andrés en su artículo PRUEBAS DE PENETRACIÓN O PENT TEST[31], los ethical hackers son personas o redes de computadoras que se dedican a analizar/evaluar las debilidades o vulnerabilidades de los sistemas informáticos, atacándolos con autorización de sus propietarios, para así poder encontrar alguna falla que los hackers o piratas puedan utilizarlos, es por eso que surge la necesidad de desarrollar esto que se conoce como pruebas de penetración o Pent Test. Las pruebas de penetración o Pent Test son un conjunto de metodologías y técnicas que permiten realizar una evaluación integral de las debilidades de los sistemas informáticos. Estas pruebas son realizadas con el consentimiento del o los propietarios de los sistemas, y es obligatorio y aconsejable que esto lo realicen personas ajenas a la empresa, ya que si lo hiciera alguien de la empresa se cometería el error de ser juez y parte.

[30] VOUTSSAS Juan. Preservación documental digital y seguridad informática Op. Cit.
[31] RAMOS RAMOS Jorge Luis. PRUEBAS DE PENETRACIÓN O PENT TEST, En: Revista de Información, Tecnología y Sociedad, No. 8 (Jun, 2013); pp. 31-33.

Por último, en la revista electrónica de Computación Informática Biomédica y Electrónica aparece el artículo Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web de Hernández Saucedo, Ana Laura y Mejía Miranda, Jezreel[32] de la ciudad de México donde expone que en la actualidad el riesgo para los sistemas informáticos ha aumentado debido a un crecimiento en la complejidad en las tecnologías de la información. Hoy en día cualquier computadora conectada a internet está expuesta a diversas amenazas. Una consecuencia es el aumento en el número de ataques informáticos. Una manera de prevenirlo es actuar anticipadamente, detectando las vulnerabilidades potenciales que pueden ser aprovechadas por los atacantes. De esta manera se disminuye la probabilidad de éxito de los ataques realizados. Este trabajo revisa algunas de las técnicas y herramientas utilizadas actualmente para la detección de vulnerabilidades, se presenta una matriz de trazabilidad entre ataques, vulnerabilidades, técnicas y herramientas que determinarán cuales vulnerabilidades y ataques pueden ser mitigadas con la utilización de dichas técnicas y herramientas.

[32] HERNÁNDEZ SAUCEDO, Ana Laura; MEJIA MIRANDA, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web, En: Revista electrónica de Computación, Informática Biomédica y Electrónica, Vol. 4 No. 15 (Feb, 2015).

4.4 MARCO LEGAL O JURÍDICO

Legislación de Seguridad Informática en Colombia

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001[33]

Según la Ley NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001, establece normas que han sido elaboradas para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos.

[33] NORMA ISO 27001. “Sistema de Gestión de la Seguridad de la Información”. {En línea}. {05 Diciembre de 2017}.Disponible en http://www.gesconsultor.com/iso-27001.html

5 DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación empleado es exploratoria, al sistema de información, se ejecutará un proceso de evaluación con el fin de identificar vulnerabilidades en el sistema de información, y aplicada debido a que con los hallazgos se propone una solución según las normas y técnicas de la seguridad informática.

5.2 METODO DE INVESTIGACION

Para este proyecto aplicado se usará la norma ISO IEC 27001 (2006), la cual da una variedad de controles para evaluar los riesgos asociados a la seguridad de la información, donde se evalúa las vulnerabilidades en el Sistema de gestión de la seguridad de la información de la empresa taller industrial Alkan S.A. Se aplicara el modelo MAGERIT [34]que nos permitirá analizar y gestionar los riesgos de sus sistemas, la evaluación de riesgos se establece al seleccionar los objetivos de control y los controles a ser revisados, la medición realizada se fundamentara en los porcentajes de cumplimiento: Menos del 50% del control se considera riesgo de vulnerabilidad latente y mayor del 50% se considera de tratamiento adecuado y no manifiesta existencia de vulnerabilidades relevantes para la seguridad de la información. El proceso metodológico comprende los siguientes pasos:

1. Identificar y aceptar el riesgo. Admitir el riesgo latente y seguir trabajando, o establecer controles para aminorar el riesgo a un estado admisible.

2. Prevenir el riesgo. Suprimir el origen y/o secuela del riesgo.

3. Disminuir el riesgo: Restringir el riesgo con el establecimiento de controles que disminuyen el efecto perjudicial de una amenaza que aprovecha una debilidad.

[34] MOLINA MIRANDA, María Fernanda. PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL. Madrid. 2015, 89. Trabajo fin de master. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en http://www.dit.upm.es/posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Opciones de tratamiento del riesgo: mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Disminuir la desvalorización ocasionada por una amenaza.
- Aminorar la posibilidad de que una amenaza se realice.

En los casos anteriores se debe aumentar u optimizar el grupo de protecciones.

Proteger los recursos de los sistemas de información del taller industrial Alkan S.A y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

5.3 FUENTES Y TÉCNICAS DE RECOLECCION DE INFORMACION

Para el desarrollo del pentesting se utilizará solo la fuente primaria.

5.3.1 Fuentes primarias

La primera fuente de información será a través de las visitas a las instalaciones de la red de la empresa taller industrial Alkan S.A.S, mediante el contacto con el personal de sistemas. La recolección de la información será mediante entrevistas, cuestionarios y listas de chequeo, las cuales permitirán conocer el estado de la red de la empresa.

5.4 DELIMITACIÓN Y ALCANCE

El proyecto se llevará a cabo en los sistemas operativos y base de datos de la empresa taller industrial Alkan S.A.S. ubicada en la ciudad de Guadalajara de Buga – Valle del Cauca.

Para la aplicación del proyecto se tendrán en cuenta herramientas de pentesting; la metodología a trabajar será penetración Kali Linux, posteriormente se aplicarán pruebas de penetración que sirvan de evidencia y posibles amenazas existentes en los sistemas operativos y base de datos de la empresa.

5.5 TÉCNICAS E INSTRUMENTOS

Para esta investigación y la realización del pentesting, se tiene previsto utilizar las siguientes herramientas y técnicas:

- Visitas técnicas: Se realizarán visitas técnicas para verificar aspectos físicos y administrativos de la red.
- Entrevistas al encargado de sistemas y a los usuarios de la red de datos
- Cuestionarios aplicados a los usuarios y encargado de sistemas.
- Listas de chequeo para determinar que controles existen dentro de la seguridad en la red.
- Pruebas de Penetración: se realizarán pruebas para identificar vulnerabilidades de la red.

5.6 POBLACIÓN Y MUESTRA

La población lo conforman los usuarios que integran la planta de trabajo y que se conectan a la red de la empresa taller industrial Alkan S.A.S.

Para la muestra se seleccionará solamente al personal encargado del departamento de sistemas.

6 METODOLOGIA DEL DESARROLLO DEL PROYECTO

A continuación, se muestran las actividades a realizar para conseguir el desarrollo de cada objetivo propuesto:

6.1 PLAN DE DESARROLLO FASE 1

Objetivo 1: Realizar el levantamiento de los activos de información de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle mediante la metodología Magerit.

- Realizar visitas técnicas para conocer la infraestructura de la red de datos de la empresa y activos.

6.1.1 Plan de desarrollo para la fase 2

Objetivo 2: • Aplicar pruebas de penetración a la red de datos empleando la metodología del ethical hacking con la herramienta Kali Linux para diagnosticar las vulnerabilidades de seguridad de la información de la empresa Taller Alkan de la ciudad Guadalajara de Buga, Valle.

- Realizar un plan de pruebas de penetración, usando de las herramientas de Kali Linux[35] y Nmap[36] donde se escogerán las más relevantes que se acojan al caso del proyecto con el fin de determinar vulnerabilidades, riesgos y amenazas existentes en la seguridad de la red de la empresa taller industrial Alkan S.A.S.

[35] Kali Linux. Nuestra distribución más avanzada de pruebas de penetración en https://www.kali.org/
[36] Nmap. Disponible en https://nmap.org/

6.1.2 Plan de desarrollo para la fase 3

Objetivo 3: Valorar las vulnerabilidades encontradas según los riesgos detectados en las pruebas de testeo de red y su efecto en el sistema de información.

- Realizar un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados y las pruebas de penetración.

6.1.3 Plan de desarrollo para la fase 4

Objetivo 4: Plantear estrategias de reducción de los riesgos encontrados para evitar y reforzar la seguridad de la información.

- Examinar y recopilar la información y los resultados obtenidos en las pruebas de pentesting.
- Presentar el informe de pentesting a la oficina de sistemas y la dirección de la empresa Taller industrial Alkan S.A.S.

7 LEVANTAMIENTO DE LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA TALLER INDUSTRIAL ALKAN S.A.S

A continuación, se identificaron los siguientes activos en la empresa Taller Industrial Alkan S.A.S tomando como base la metodología MAGERIT Versión 3. La cual nos define la clasificación de activos. Magerit.

Tabla 1. Activos de la empresa

ACTIVO	CANTIDAD
(P) PERSONAL	
(IS) Ingeniero de sistemas	1
(L) INSTALACIONES	
(SP) sede principal	1
(COM) SISTEMA DE COMUNICACIÓN	
(ComT)Teléfono Panasonic	1
(E)EQUIPO	
(CE) Computador de escritorio	1
(SW) Software	5
(I) Impresora	1
(C) Comunicación	1
(U) UPS	1
(HW) Hardware	4
(OE) Otros Equipos	1

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 2. Descripción del activo

TIPO	NOMBRE DEL ACTIVO
(P)PERSONAL	(IS) INGENIERO DE SISTEMAS
	Profesionales del área de ingeniería de sistemas con tarjeta profesional vigente, conocimientos de base de datos y web. Persona proactiva, creativa, organizada y con experticia técnica en su trabajo
(L)INSTALACIONES	(SP) SEDE PRINCIAL
	Local propio de 1 planta, ubicado en la Carrera 24 # 13 - 04, Barrio Sucre, Guadalajara de Buga, Valle del Cauca, Colombia
(COM) SISTEMA DE COMUNICACION	(COMT)TELÉFONO PANASONIC
	DESCRIPCION: Panasonic KX-TGF382 Dect 6.0, frecuencia de 1.9GHz libre de interferencias, Base principal con su auricular y 2 auriculares, cuenta con contestadora digital integrada con hasta 18 minutos de grabación UBICACIÓN departamento de sistemas, cantidad 1
(E) EQUIPO	(CE) COMPUTADOR DE ESCRITORIO
	Referencia: Intel Inside Core i7 a 2.30 Ghz, 1 Tera de disco duro y 16 GB de memoria RAM. Ubicados en: departamento de sistemas
	(SW) SOFTWARE
	Windows 10, Office 2016, MySQL
	(I) IMPRESORA
	HP LaserJet p1102w
	(C) COMUNICACIÓN
	Referencias: Radio Walkie Talkie, Celulares (Iphone 5s, Motorola g5), Teléfono Inalámbrico. Ubicados en: departamento de sistemas y gerencia

Tabla 2. Continuación

	(U) UPS
	Referencia: Powercom, Ubicado: departamento de sistemas.
	(HW) HARDWARE
	Referencia: Memoria RAM, Disco Duro Hitachi portable. Ubicado: departamento de sistemas.
	(OE) OTROS EQUIPOS
	Referencia: Cámara Digital, Scanner Ubicados: Departamento de sistemas

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

7.1 DEPENDENCIAS ENTRE ACTIVOS

Instalaciones (SP) Sede Principal Valoración Extremo. Es el centro de operaciones de la compañía, es donde todo el personal realiza sus labores cotidianas, es donde se guardan todos los materiales de trabajo, donde se desarrollan todas las tareas administrativas y donde se almacena toda la información vital dentro de esta, así que guarda una estrecha relación con cada una de los departamentos de esta, y es uno de los pilares vitales dentro de la empresa.

(CE) Computador de escritorio: Valoración Alto. Los equipos de cómputo distribuidos dentro de la compañía prestan un soporte a las tareas tanto administrativas, comerciales y técnicas que se desarrollan en esta, como tal brindan las herramientas de trabajos necesarias para los elementos de talento humano, la parte administrativa y técnica. Igualmente, estos sirven como medio para acceder a información, para establecer tareas de tipo administrativo, control de empleados, y trabajos en curso prestados por la compañía.

(SW) Software: Valoración Medio. Dentro de la compañía existen elementos de software de tipo general, como las suites ofimáticas, que es utilizado de forma constante dentro de la empresa, hay que tener en cuenta que una falla de este software puede desembocar en problemas de tipo interno, para lo cual se necesitan establecer un modelo de respaldo, que permita restablecer la información requerida ante cualquier fallo.

(I) Impresora Valoración Bajo. Las impresoras prestan un servicio dentro de la compañía que, si bien es necesario en labores diarias, su daño no representa un riesgo alto para el funcionamiento de la compaña, y no suele tener un costo alto dentro de la información o labores vitales dentro de esta.

(C) Comunicación Valoración Media. Es parte importante dentro de todos los departamentos y uno de los medios de comunicación con el cliente, pero la facilidad que se tiene actualmente para establecer canales de información que van desde internet, teléfonos celulares y demás, por lo cual una falla en este sistema

no supondría un daño tan grande dentro de la compaña y tampoco tendría un impacto directo dentro de sus actividades cotidianas, más partiendo de la naturaleza de la compañía.

(U) UPS Valoración Alta (Heredado). Permiten establecer un medio de protección frente a la información que se trabaja en los equipos de cómputo de la compañía, permitiendo guardar la información que se está trabajando en ellos en momentos de fallas eléctricas.

(HW) Hardware Valoración Alta (Heredada). Disco duro de respaldo utilizado para contingencias dentro de la empresa, contiene información vital de la compañía que brinda un medio de soporte ante problemas de tipo físico, por ello es importante contar con como medio de respaldo.

(OE) Otros Equipos Valoración Bajo. Estos brindan soporte sobre tareas rutinarias dentro de varios departamentos de la empresa, pero no contienen información relevante dentro de la compañía, ni brindan soporte vital a ningún proceso específico

7.2 VALORACIÓN DE LOS ACTIVOS. EN ESTA ACTIVIDAD PARA REALIZAR LA VALORACIÓN DEL ACTIVO SE REALIZÓ DE ACUERDO A LA METOLOGIA MARGERIT V .3 CON LAS SIGUIENTES DIMENSIONES.

Tabla 3. Valorización de los activos

DIMENSIONES
[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de la Información.
[A] Autenticidad
[T] trazabilidad

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 4. Criterio de valoración de activos

Valor		***Criterio***
Puntuación	Concepto	
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 – 8	Alto	Daño grave
3 – 5	Medio	Daño importante
1 – 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 5. Identificación de activos

		DIMENSIONES				
NUMERO DE ACTIVO	ACTIVO IDENTIFICADO	(D)	(I)	(C)	(A)	(T)
(P) PERSONAL						
1	(IS)Ingeniero de Sistemas	5	6	8	2	6
(L) INSTALACIONES						
2	(SP) Edificio Sede Principal	9	7	8	0	0
SISTEMAS DE COMUNICACIÓN						
16	(COM) TELEFONOS PANASONIC	4	0	5	0	0
(E) EQUIPO						
21	(CE) Computador de escritorio	8	7	8	6	5
23	(SW) Software	5	9	9	9	4
24	(I) Impresora	2	1	0	0	0
25	(C) Comunicación	3	3	7	2	2
26	(U) UPS	4	3	1	8	4
30	(HW) Hardware	5	3	4	1	3
31	(OE) Otros Equipos	4	3	5	5	3

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

7.3 CARACTERIZACIÓN Y VALORACIÓN DE LAS AMENAZAS

Estas amenazas se han tomado de los elementos de la metodología Magerit V3.

Clasificación de amenazas.

Tabla 6. Clasificación de amenazas

Código	Nombre
[N]	Desastres naturales
[I]	De origen industrial
[E]	Errores y fallos no intencionados
[A]	Ataques intencionados

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 7. Identificación de amenazas

Activo	**Amenazas**
(P)PERSONAL **(IS)Ingeniero de sistemas**	[E7] Deficiencias en la organización [E19] Fugas de información [E28] Indisponibilidad del Personal • 42-Daño a la disponibilidad del personal [A29] Extorsión [A30] Ingeniería social
(L) INSTALACIONES **(SP) Edificio Sede Principal**	[N1] Fuego • incendio [N2] Daños por agua • inundaciones [N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación [I1] Fuego • Incendio [I2] Daños por agua • Escapes • Fugas [E19] Fugas de información [A7] Uso no previsto [A26] Ataque destructivo
Equipamiento informático	
((DVRC))	(N.1) Fuego
(CTMX)	(N2) DAÑOS POR AGUA

Tabla 7. (Continuación)

(CTMX)	**[N.*] DESASTRE NATURALES**
(CTMX)	[I.5] Avería de origen físico o lógico
(DVRC)	[A.23] Manipulación de los equipos.
TELEFONIA **(COM) Teléfonos Panasonic**	[N1] Fuego • incendio [N2] Daños por agua • inundaciones [N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación • [E19] Fugas de información [I1] Fuego • Incendio [I2] Daños por agua • Escapes • Fugas [A26] Ataque destructivo
(E) EQUIPO **(CE) Computador de escritorio** **(SW) Software** **(I) Impresora** **(C) Comunicación** **(U) UPS** **(HW) Hardware** **(OE) Otros Equipos**	[N1] Fuego • incendio [N2] Daños por agua • inundaciones [N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación [E19] Fugas de información [I1] Fuego • Incendio [I2] Daños por agua • Escapes • Fugas [A26] Ataque destructivo [E19] Fugas de información

Tabla 8. Catálogo de elementos

Valor			**Criterio**
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 9. Valorización de amenazas

Valor	**Criterio**	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable de activo
50%	M	Degradación MEDIANA considerable de activo
10%	B	Degradación BAJA considerable de activo
1%	MB	Degradación MUY BAJA considerable de activo

Fuente Magerit 2.3 – Libro II – Catalogo de elementos

Tabla 10. Probabilidad de ocurrencia

Valor		**Criterio**	
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 11. Degradación del valor

Valor	***Criterios***	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 12. Dimensión de seguridad

Activo	**Amenaza**	**Frecuencia**	**DIMENSION DE SEGURIDAD**				
			D	I	C	A	T
(P) PERSONAS	E7] Deficiencias en la organización	F	M	-	-	-	-
	[E19] Fugas de información	F	-	-	B	-	-
	[E28] Indisponibilidad del Personal • 42-Daño a la disponibilidad del personal	PF	B	-	-	-	-
	[A29] Extorsión	PF	B	B	B	-	-
	[A30] Ingeniería social	MA	B	B	B	-	-
(L) INSTALACIONES	[N1] Fuego • Incendio	PF	B	-	-	-	-
	[N2] Daños por agua • Inundaciones	PF	A	-	-	-	-
	[N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación	PF	A	-	-	-	-
	[I1] Fuego • Incendio	PF	A	-	-	-	-

Tabla 12. (Continuación)

	[I2] Daños por agua • Escapes • Fugas						
	• [E19] Fugas de información	PF	A	-	-	-	-
	[A7] Uso no previsto	FN	M	-	M	-	-
	[A26] Ataque destructivo	MF	MA	MA	MA	-	-
	[A26] Ataque destructivo	FN	B	-	-	-	-
EQUIPAMIENTO INFORMATICO							
((DVRC))	(N.1)Fuego	PF	MA	MA	MA	MA	MA
(CTMX)	(N2) DAÑOS POR AGUA	PF	B	B		B	
(CTMX)	[N.*] DESASTRE NATURALES	PF	M	M	M	M	M
(CTMX)	[I.5] Avería de origen físico o lógico	PF	M	M	M	M	M
(DVRC)	[A.23] Manipulación de los equipos.	FN	MA	MA	MA	MA	MA
Comunicaciones	[N1] Fuego • Incendio	PF	A	-	-	-	-
	[N2] Daños por agua • Inundaciones	PF	A	-	-	-	-
	[N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación	PF	A	-	-	-	-
	[I1] Fuego • Incendio	PF	A	-	-	-	-
	[I2] Daños por agua • Escapes • Fugas	PF	A	-	-	-	-
	[A26] Ataque destructivo	FN	M	-	-	-	-
	[E19] Fugas de información						

Tabla 12. (Continuación)

EQUIPOS DE INTERCAMBIO DE DATOS	[A.11] Acceso no autorizado	MF	-	MA	MA	-	-
	[A.26] Ataque destructivo	MF	MA	-	-	-	-
	[A.25] Robo	MF	MA	-	MA	-	-
	[I.5] Avería de origen físico o lógico • Entorno (accidental) • Humano (accidental o deliberado)	F	A	-	-	-	-
	[I.6] Corte del suministro eléctrico • Entorno (accidental) • Humano (accidental o deliberado)	FN	MA	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad • Entorno (accidental) • Humano (accidental o deliberado)	MF	A	-	-	-	-
	[I.1] Fuego • Entorno (accidental)	FN	A	-	-	-	-
	[N1] Fuego • Incendio	FN	A	-	-	-	-
	[N2] Daños por agua • inundaciones	PF	MA	-	-	-	--
	[N.*] Desastres naturales • 04 - SINIESTRO MAYOR • 06 - FENÓMENO CLIMÁTICO • 07 - FENÓMENO SÍSMICO	PF	A	-	-	-	-
	[I.4] Contaminación electromagnética • 14 - EMISIONES ELECTROMAGNÉTICAS	FN	M	-	-	-	-
(E) EQUIPO	[N1] Fuego • Incendio	PF	M	-	-	-	-
	[N2] Daños por agua • Inundaciones	PF	-	-	B	-	-

Tabla 12. (Continuación)

	[N*] Desastres naturales • **04-Siniestro mayor** • **06-Fenómeno climático** • **07-Fenómeno Sísmico** **10-Inundación**						
	[N1] Fuego • Incendio	PF	B	-	-	-	-
	[N2] Daños por agua • Inundaciones	PF	B	B	B	-	-
	[N1] Fuego • Incendio	PF	B	B	B	-	-
	[N2] Daños por agua • Inundaciones	PF	B	-	-	-	-
	[N*] Desastres naturales • 04-Siniestro mayor • 06-Fenómeno climático • 07-Fenómeno Sísmico • 10-Inundación	PF	A	-	-	-	-
	[I1] Fuego • Incendio	PF	A	-	-	-	-
	[I2] Daños por agua • Escapes • Fugas	PF	A	-	-	-	-
	• [E19] Fugas de información	PF	A	-	-	-	-
	[A7] Uso no previsto	FN	M	-	M	-	-
	[A26] Ataque destructivo	MF	MA	MA	MA	-	-

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

7.4 JUSTIFICACIÓN DE AMENAZAS – EQUIPAMIENTO INFORMÁTICO

(DVRC) (N.1) Fuego: se consideró el impacto de daño muy grave en todas las dimensiones ya que si llega ocurrir el fuego se perdería toda la infraestructura física y equipos hardware y maquinaria de producción que brindan el soporte a otros activos en la compañía y comparten información de seguridad física tanto externa como internamente

(CTMX)(N2) DAÑOS POR AGUA. El impacto se consideró con poca frecuencia y baja disponibilidad este activo se encuentra como si ocurre la catástrofe no afecta mucho a la compañía

(CTMX)[I.5] Avería de origen físico o lógico: en la degradación es poco frecuente que ocurra y en las dimensiones de que sea manipulada es media

(DVRC)[A.23] Manipulación de los equipos este tipo de amenaza es muy alta en todas las dimensiones ya que con una manipulación de los este equipo se pueden presentar robos dentro de la organización o que procedimiento en producción no sean controlados o vigílalos

(SEI) EQUIPOS DE INTERCAMBIO DE DATOS- [A.11] Acceso no autorizado, [A.26] Ataque destructivo, [A.25] Robo: Los computadores se encuentra en un lugar de libre acceso sin ningún tipo de control de ingreso para los usuarios.

Daños provocados por ataques informáticos, partiendo de la pobre configuración de los computadores, estos no se encuentran encriptados. [I.5] Avería de origen físico o lógico, [I.6] Corte del suministro eléctrico: Los computadores no se encuentran en locaciones dedicadas, es decir, están ubicados en oficina multi propósito esto puede llevar a una mala manipulación por el personal que utiliza esas oficinas a diario o por parte del personal de aseo. [I.4] Contaminación electromagnética, [I.1] Fuego, [I.7] Condiciones inadecuadas de temperatura o humedad: Los computadores no se encuentran en una locación dedicada que permita establecer las condiciones óptimas de temperatura, humedad y suciedad. [N1] Fuego, [N2] Daños por agua, [N.*] Desastres naturales: Daños causados por accidentes o desastres naturales.

7.5 ESTIMACIÓN DEL ESTADO DE RIESGO

Los activos con calificación Media deberán ser evaluados otra vez para cambiar o utilizar nuevos controles, los de calificación Alta y muy alta deberán ser objeto de atención Urgente.

7.6 ESTIMACIÓN DE IMPACTOS

Tabla 13. Escala de colores

Valor	Criterio
10	Crítico
9-8	Muy Alto
7-6	Alto
5-4	Medio
3-2	Bajo
1-0	Despreciable

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 14. Impacto

	DIMENSIONES				
ACTIVO IDENTIFCADO	(D)	(I)	(C)	(A)	(T)
(P) Personal					
(IS)Ingeniero de Sistemas	5	6	10	3	2
(L) Instalaciones					
(SP) Edificio Sede Principal	6	6	7	0	0
(COM) Redes de comunicación					
(COM) TELEFONOS PANASONIC	3	1	3	0	0
(E) EQUIPO					
(CE) Computador de escritorio	3	3	3	3	2
(SW) Software	6	8	5	6	4

Tabla 14. (Continuación)

(I) Impresora	3	2	3	1	0
(C) Comunicación	6	3	4	3	2
(U) UPS	10	10	4	3	4
(HW) Hardware	9	9	4	8	5
(OE) Otros Equipos	2	2	2	0	0

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

7.7 ESTIMACIÓN DE RIESGOS

Tabla 15. Estimación de riesgos

Valor	Criterio
10 – 9	Crítico
8 – 6	Grave
5 – 3	Apreciable
2 - 0	Asumible

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

Tabla 166. Estimación de riesgos activos

	DIMENSIONES				
ACTIVO IDENTIFCADO	(D)	(I)	(C)	(A)	(T)
(P) Personal					
(IS)Ingeniero de Sistemas	2	3	5	2	1
(L) Instalaciones					
(SP) Edificio Sede Principal	5	3	3	1	1

Tabla 16. (Continuación)

(COM) Redes de comunicación					
(COM) TELEFONOS PANASONIC	1	1	1	0	0
(E) EQUIPO					
(CE) Computador de escritorio	3	3	3	2	3
(SW) Software	4	4	4	3	3
(I) Impresora	0	0	0	0	0
(C) Comunicación	1	1	1	0	0
(U) UPS	1	1	1	1	1
(HW) Hardware	4	4	4	3	3
(OE) Otros Equipos	0	0	0	0	0

Fuente: Magerit V.3, Libro II, Catálogo de Elementos

8 RESULTADOS

APLICACIONES ELEGIDAS

Para este proyecto se eligió el sistema Kali Linux por tener aplicaciones gratuitas que ayudan a explotar vulnerabilidades de forma fácil y práctica, ayudando a identificar las vulnerabilidades que puedan afectar el sistema operativo y bases de datos del Taller industrial Alkan S.A.S. De estos programas se tiene:

Nmap: Aplicación que permite auditar las redes, muestra los puertos abiertos de forma rápida y aplicaciones que corran sobre estos[37].

Metasploit: Sirve para explotar las vulnerabilidades de las bases de datos.

Ms08-67: Se trata de una vulnerabilidad para la ejecución remota de código. Un atacante que aprovechara esta vulnerabilidad podría tomar el control completo de un sistema afectado de forma remota. En los sistemas basados en Microsoft Windows 2000, Windows XP, Windows 7 y Windows Server 2003, un atacante podría aprovechar esta vulnerabilidad sobre RPC (Remote Procedure Call – Llamada a Procedimiento Remoto) sin autenticación y ejecutar código arbitrario.[38]

Hombre en el medio (Man In-The-Middle): Ataques de interceptación de tráfico, donde se suplanta el direccionamiento bien sea físico o IP con la herramienta Ettercap incluida en el Kali Linux.[39]

---

[37] Nmap. Op. Cit.

[38] Soporte Técnico de Microsoft. Disponible en Internet: https://support.microsoft.com/es-co/help/958644/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execu

[39] Ministerio de las TIC – MINTIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Nessus: Permite identificar las debilidades y errores de configuración que pueden ser usadas para ataques múltiples.

SqlMap: Utilizada para inyección Sql para así obtener listas y registro de la base de datos.

Wireshark: es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica.

8.1 CONFIGURACION DEL SISTEMA PARA PRUEBAS

Se provee el Hardware y Software para la realización de las pruebas de pentesting realizadas a la empresa Taller Industrial Alkan S.A.S para el desarrollo del proyecto:

1. Características del equipo para realizar las pruebas: Disco duro 1 Tera, Ram 16 GB, procesador Intel I7.

2. Sistema operativo Kali Linux de 64 Bits con el cual usa sus poderosas herramientas para identificar vulnerabilidades en el sistema operativo y bases de datos de la empresa. La descarga se hace de la página oficial https://www.kali.org/.

3. Kali Linux se instaló en la máquina virtual VMWare de caracteristicas memoria Ram 4 GB, 20 Gigas de disco duro, procesador 2 Corel. Se descargó de la página oficial https://www.vmware.com/co.html.

8.2 PLAN DE PRUEBAS

Para hallar las vulnerabilidades del sistema operativo y bases de datos de la empresa Taller Industrial Alkan se apoyó en un plan de pruebas con las aplicaciones seleccionadas:

1. Recopilación de información sobre la aplicación

a) Reconocimiento de la aplicación para identificar la magnitud y alcance
b) Nombre de la aplicación
c) Función de la aplicación
d) Licencia de la aplicación
e) Registro de la aplicación
f) Fácil manejo de la aplicación
g) Necesidades para su manejo

2. Análisis estático

a) Identificación de vulnerabilidades de la aplicación seleccionada
b) Configurar permisos sobre el sistemas operativo a procesar
c) Analizar con que herramienta se va a trabajar en cada paso a ejecutar
d) Configurar acceso a la red y base de datos

3. Análisis dinámico

a) Identificación de vulnerabilidades de la aplicación usada en cada proceso
b) Instalar configuración y uso de la aplicación
c) Identificación de la red a vulnerar
d) Identificación de la base de datos

8.3 RESULTADOS OBTENIDOS EN LA EJECUCION DE LAS PRUEBAS

Después de instalar y configurar el plan de pruebas, se ejecuta el plan de pruebas de seguridad a las aplicaciones seleccionadas. Estos resultados se encuentran en el anexo 1.

8.4 ANALISIS DE RESULTADOS

Al finalizar el plan de pruebas de cada aplicación de la seguridad de la empresa Taller Alkan S.A.S, los resultados se ordenan y se analizan de la siguiente manera:

1. El acceso al área de informática y entorno físico no tiene ninguna restricción, esto se da porque cualquier empleado de la empresa puede acceder a esta área donde está el sistema operativo y la base de datos de la empresa.

2. El ingreso al computador del personal de la empresa tiene claves alfanuméricas de más de ocho (8) dígitos haciendo seguro este proceso, pero se observa que los empleados dejan los computadores abiertos ocasionando que se pueda acceder a información valiosa, no cierran los programas en horas de descanso.

3. Al utilizar la aplicación Nmap de Kali Linux se identificaron puertos abiertos de comunicación, las aplicaciones que están ejecutando. Una persona de la empresa o ajena con buenos conocimientos de informática puede sacar provecho de esto. Ver anexo 2.

4. La asignación de los puertos se encuentran reglamentados por la agencia de asignación de números de internet IANA[40]. Esta asignación la hacen mediante tres rangos donde se encontró puertos reservados, registrados y privados. Estos puertos son necesarios para que los sistemas funcionen, la empresa es descuidada con los Firewall, no tienen en cuenta el vencimiento de esta herramienta, no han implementado un sistema con Snort[41] que informe en tiempo real cualquier ataque. Ver anexo 3.

5. La aplicación SQLMAP se usó para penetración en la base de datos encontrando que no se ha implementado los tipos de seguridad para esta, un empleado, exempleado, persona externa con buenos conocimientos de informática puede acceder a esta y provocar daños.

6. Con la aplicación Nessus se identificó errores de configuración del sistema operativo, puertos por los cuales pueden acceder para vulnerar, fallos de software instalado. Esa aplicación da un informe detallado de lo que hace cada vulnerabilidad y como podría solucionarse el error o falla del sistema, además las categoriza en rangos de bajo nivel, medio o alto.

[40] IANA, Agencia de Asignación de Números de Internet [en línea], [diciembre 2017]. Disponible en Internet: https://www.iana.org/
[41] Snort. Sistemas de Detección de intrusos [en línea], diciembre2017]. Disponible en Internet: https://www.snort.org/

9 PERSONAS QUE PARTICIPAN EN EL PROCESO

En el desarrollo del presente proyecto para la empresa Taller Industrial Alkan S.A.S. en su culminación del proceso, se necesitó de personas con las cuales se tuvo interacción para poder llevarlo a cabo y lograr su totalidad de lo planteado.

El rol de investigador, que es la persona encargada de hacer toda la investigación, consultas e informe sobre el desarrollo de todo el proyecto, además de tener el rol de director que es el encargado de guiar y dirigir al investigador de la ruta que debe tomar el proyecto y delimitaciones sobre el mismo.

9.1 PROPONENTES PRIMARIOS

Investigadores: Adrián Pastrana Franco nació en Colombia – Guadalajara de Buga, el 27 de Marzo de 1980. Egresado del programa de Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia UNAD. Durante el año 2015, se desempeña como Docente de Informática de la Institución Educativa Narciso Cabal Salcedo de Guadalajara de Buga.

Javier Marmolejo Serrano nació en Colombia – Palmira, el 09 de Febrero de 1.966 Se graduó de la Universidad Nacional Abierta y a Distancia –UNAD– en Ingeniería de Sistemas y de la Universidad del Valle en Tecnología de Sistemas de Información, es estudiante Universidad UNAD de la especialización en Seguridad Informática.

9.2 PROPONENTES SECUNDARIOS

Ing. Alex Fernando Trujillo Plaza nació en Colombia – Buga, el 05 de Diciembre 1984, se graduó de la Universidad Uniciencia en Ingeniería de Sistemas, actualmente trabaja como el administrador de sistemas de la empresa Taller Industrial ALKAN S.A.S.

Tutor: Ing. Juan José Cruz Garzón Profesional de Servicios y tecnología de la información, Seguridad Informática y Gestión en Proyectos

Director de proyecto: Mg. Yina Alexandra González Sanabria magister en Tecnologías de La Información Aplicadas a La Educación

10 RECURSOS NECESARIOS PARA EL DESARROLLO

10.1 RECURSO HUMANO

El proyecto lo llevaran a cabo en su totalidad los estudiantes de la especialización en seguridad informática Javier Marmolejo Serrano y Adrián Pastrana Franco, en un lazo de 14 semanas aproximadamente.

10.2 RECURSO MATERIALES Y FINANCIERO

En la siguiente tabla se describe el recurso físico y financiero que se requiere para llevar a cabo el proyecto, igualmente se ilustra la fuente de financiación.

Recurso material y financiero

Tabla 177. Recurso material y financiero

Cantidad	Recurso Material	Valor
Recurso tecnológico		
1	Equipo de cómputo, Core i7-4790 3.60 GHz, 8 Gb en RAM, 1 Tera en Disco duro	$3.299.000
1	Impresora HP LaserJet P1102w	$450.000
1	Tóner Impresora	$380.000
1	Disco Duro externo de 500 GB	$180.000
1	Internet	$220.000
	Subtotal	$4.529.000
Recurso material		
1	Papelería	$80.000
	Subtotal	$80.000
	Total Recurso Financiero	$4.609.000

Fuente: El autor.

10.3 RECURSO TÉCNICO

Herramientas de Pentesting: Nmap, Metasploit, Ettercap, SQLmap, Kali Linux, Wireshark.

10.4 RECURSO INSTITUCIONAL

El desarrollo de este proyecto de pruebas de penetración a la infraestructura tecnológica de la empresa taller industrial ALKAN S.A.S. de la ciudad Guadalajara de Buga, Valle para identificar vulnerabilidades contará con el apoyo de los recursos de la institución UNAD, investigación de libros de la biblioteca institucional para dar soporte a la investigación, uso eficiente de los equipos de laboratorio.

11 INFORME DE VULNERABILIDADES Y RECOMENDACIONES

La red de la empresa Taller industrial Alkan S.A.S., no presenta ningún grado de complejidad para la administración y control de seguridad informática. A continuación, se presentan las vulnerabilidades y recomendaciones que se le sugieren a la empresa para mejorar su seguridad en sus sistemas operativos y base de datos.

ADMINISTRATIVAS Y PERSONAL DE LA EMPRESA

Concientizar a los empleados de la empresa de la importancia que tiene la manipulación y confidencialidad de la información: Los funcionarios y empleados adquieren las responsabilidades y cuidados que se deben tener al manipular información confidencial de la empresa.

Todas las claves y privilegios que tienen los empleados de la empresa deben ser bloqueados a la hora que se termine el contrato de forma definitiva: En caso que el contrato termine en malos términos se debe impedir que el afectado despedido manipule la información.

Prohibir cualquier actividad de personal no autorizado en las áreas donde hay información y acceso a los equipos de cómputo: Se evitará daños en los equipos ya sea por derramamiento de líquidos o comida sobre ellos provocando la pérdida del equipo y de la información, además se evitará que personal no autorizado pueda acceder a la información de los usuarios.

Los empleados de la organización que ejercen funciones en los sistemas de información deberán ser capacitados periódicamente en materia de seguridad: El departamento de seguridad informática deberá difundir las políticas de seguridad implementadas por la empresa a todos los empleados en general.

Los usuarios de la empresa que tienen correo electrónico deberán conocer la importancia del uso del mismo, ya que, si no le damos un buen uso, se puede ser víctima de virus por descargas de archivos adjuntos: Los empleados deberán tomar conciencia del uso del correo electrónico, del riesgo a que están expuestos por el mal uso del mismo, solo se deberá utilizar para intercambiar información exclusiva de la empresa.

Es necesario que los empleados tengan claro los aspectos de integridad, disponibilidad y confiabilidad de los bienes y servicios de la entidad: Los empleados deberán adquirir el compromiso al momento de ser contratados de proteger y salvaguardar los activos informáticos, ya que es lo más valiosos que posee la organización y así se evitaran fugas de información.

BASE DE DATOS

Los resultados de las pruebas en la base de datos se identificaron las siguientes vulnerabilidades:

Algunos usuarios cuentan con políticas de contraseñas débiles, permite asignar contraseñas iguales al nombre de usuario fáciles de identificar, no cuenta con la longitud mínima de caracteres, para la construcción de la contraseña, no cuenta con criterios de asignación de caracteres especiales como condición obligatoria: Se recomienda establecer políticas más fuertes en la definición de contraseñas, contar con una longitud mínima, no asignar el mismo nombre de usuario a la clave y asignar un mínimo de caracteres especiales.

Usuarios en desuso: Se requerirá contar con tareas periódicas de monitoreo de la base de datos para identificar usuarios en desuso.

La información contenida en las bases de datos deberá ser usada únicamente para asuntos relacionados con actividades de la empresa: Los funcionarios y empleados deben dar buen uso a la información de las bases de datos y no utilizarla para su beneficio personal que no tiene nada que ver con la actividad de la empresa.

Todos los datos de gran importancia deberán ser respaldados y almacenados en un lugar seguro: El departamento de sistemas deberá estar pendiente de realizar copias de respaldo de la información más importante de la empresa, ya que de esta forma se protegerá la información y en caso de desastre se pueda recuperar.

La información contenida en las bases de datos solo la podrá utilizar y modificar el personal autorizado: Se deberá crear una política de control de acceso la cual debe ser gestionada por el administrador de base de datos.

Incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas: Actualizar las bases de datos, de esta forma la empresa contara con un historial de acceso a las bases de datos de los empleados en caso de un uso inadecuado de la información.

Implementar una política que administre y controle la eliminación de información de la base de datos que ya no sea necesaria: La base de datos no se recargará con información innecesaria y serán más rápidas las consultas.

INFRAESTRUCTURA Y RED

Socializar los procedimientos de prevención y mitigación de los riesgos informáticos: Difundir las políticas de riesgos tanto a las directivas como a los empleados de las diferentes áreas de la empresa, para prevenir futuros desastre

en la red que puedan conllevar a la perdida en la información por culpa de ignorancia o desconocimiento de las políticas de seguridad informática implementada por la organización.

Cumplir con todas las políticas de seguridad establecidas por la organización: El departamento de seguridad informática está encargado, de que todos los empleados cumplan con las políticas de seguridad implementadas, para evitar riesgos informáticos, que puedan ocasionar daño a la red y fuga de su información.

Actualizar el cronograma de mantenimiento de equipos preventivo y correctivo: La empresa deberá realizar un cronograma de mantenimiento periódico a los equipos, así se evitará futuros daños en los computadores y la red será más eficiente.

Se cuenta con un antivirus que no realiza una buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso: La empresa deberá establecer un plan de protección del registro, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.), actualizando el sistema operacional y el antivirus periódicamente.

Mejorar la seguridad física, el ingreso de personal no autorizado: La empresa deberá hacer cumplir la política de control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas y personal no autorizado en las diferentes áreas de la entidad.

Los equipos que no estén en uso deberán ser almacenados en un lugar seguro donde se restrinja el acceso al personal no autorizado: Se deberán destruir los equipos almacenados y que ya no son útiles, para evitar la pérdida o sustracción de la información que pueda ocasionar daño a la entidad.

Los equipos de cómputo serán asignados a un responsable para evitar el uso inadecuado del mismo: Así se mejorará la administración y mantenimiento de los recursos informáticos de la organización.

El área de sistemas es la encargada de realizar los diferentes mantenimientos preventivo y correctivo de los quipos de cómputo: Para evitar deterioro de los equipos y una mala manipulación por personal no calificado.

Se deberá establecer controles de acceso en áreas donde se ubican los servidores y equipos de comunicación de la empresa: De esta forma se llevará un control de quien y a qué hora ingresa el personal autorizado a estas áreas.

Las contraseñas usadas para la configuración de equipos de red y telecomunicaciones deberán estar basadas en un estándar que defina aspectos

como: estructura, tiempo de validez y reusabilidad: La utilización de contraseñas fuertes y difíciles de descifrar evitara el acceso no autorizado de personal a los equipos y a la información confidencial de la empresa.

El personal que realiza trabajos de configuración de los dispositivos de red deberá poseer una certificación que avale sus capacidades: El personal que manipule, configure y repare los equipos deberán estar calificados debidamente para que no comprometan la seguridad de la red.

Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red, debidamente codificados e identificados: Facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de Red.

Los puertos que no estén en uso deberán ser bloqueados adecuadamente: De esta forma se evitarán accesos internos y externos de personal no autorizado a la red que puedan ocasionar daños y la manipulación de la información.

El acceso a Internet será restringido, solo para realizar labores propias de la empresa: Se deberán de bloquear algunas páginas de internet que no son necesarias para el desarrollo de la actividad de la empresa, para que los trabajadores no puedan acceder y empleen su tiempo más eficientemente en actividades propias de la empresa.

Deberá cifrarse la información que circule a través de la red: Evitará que personal no autorizado puedan acceder a la información confidencial que circula a través de la red y la puedan manipular en contra de la organización.

USO DEL SOFTWARE

La instalación de software en el equipo deberá ser instalado solo por el personal del área de sistemas autorizado: Los usuarios no podrán instalar programas que no sean de la organización para realizar su trabajo diario, ya que pueden poner en riesgo los equipos y la seguridad de la red de datos.

Todos los equipos deberán tener configurado la opción de cierre de sesión después de un lapso de inactividad: Se preverá que usuarios no autorizados puedan acceder, modificar o borrar información confidencial, mientras el usuario no está en su sitio de trabajo.

Se permitirá únicamente instalar software licenciado a los equipos: Se borrará el software inútil y se dará buen uso de los recursos informáticos utilizando únicamente el software licenciado, así se mejorará la seguridad de la red y se evitará la propagación de virus informáticos.

Todo software nuevo antes de ser instalado en el equipo deberá ser probado y evaluado: De esta forma se evitará un software defectuoso que pueda modificar la información o bloquee los equipos de la entidad y la red de datos será más eficiente y segura.

CONCLUSIONES

Se utilizó para el levantamiento de los activos de información de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle la metodología Magerit, logrando el inventario, clasificación de los diferentes activos de forma cualitativa y cuantitativa, cualificando los riesgos y medidas necesarias para minimizar el impacto de cualquier amenaza que llegue a materializarse.

Se aplicó en las pruebas de penetración la metodología Etical Hacking con la herramienta Kali Linux utilizando: Nmap, Wireshark, Metasploit, SqlMap y Ettercap, logrando así la materialización de las debilidades con que cuenta la información de la empresa Taller Industrial Alkan como: puertos abiertos, contraseñas débiles, información sin cifrar, equipos de fácil acceso con cuentas abiertas, con el apoderamiento total del equipo con metasploit.

Cada vulnerabilidad encontrada se valoró de acuerdo a la metodología Magerit dando como resultado una visión más específica sobre los impactos que estos pueden generar en la información de la empresa la cual es un valioso activo.

En el planteamiento de estrategias para la reducción de los riesgos encontrados la empresa debe invertir en recurso económico periódicamente para que todo el personal de la empresa reciba una adecuada capacitación y actualización en las áreas de seguridad informática y de los riesgos a que está expuesta, además de sus sistemas operativos y la base de datos. Todo el personal de la empresa tanto interno como externo que manipule información confidencial y sensible, debe comprometerse a protegerla, para evitar fugas de información, la cual pueda ser utilizada indebidamente.

Es importante que la empresa implante un sistema de monitoreo que permita ver en tiempo real lo que está ocurriendo en la red y si es posible instalar y configurar un firewall que permita detener cualquier posible ataque a las vulnerabilidades que la empresa posee para llegar a prevenir un siniestro.

La empresa debe estar más involucrada en cumplir y divulgar el cumplimiento de las políticas de seguridad implementadas por la empresa, además debe definir la forma clara los procesos y roles a las personas responsables del departamento de seguridad informática.

Se pudo dar solución al problema planteado de realizar pruebas de penetración a la infraestructura tecnológica de la empresa para identificar las vulnerabilidades del sistema operativo y base de datos de la empresa Taller Industrial Alkan S.A.S.

Se identificó que en la empresa Taller Industrial Alkan S.A.S. durante todo el proceso del proyecto se detectó que tienen vulnerabilidades, que no tienen implementado un sistema de seguridad informática (sistema operativo y base de

datos), ni en su infraestructura, en la empresa se puede hacer penetración e identificar puertos que alguien con mayor conocimiento del tema pueda aprovechar y acceder a información que es vital para la empresa.

BIBLIOGRAFÍA

SANTANA, Carlos. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En línea}. 2012. {7 Septiembre de 2012}. Disponible en https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

EcuRed. Kali Linux. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://www.ecured.cu/Kali_linux

NORMA ISO 27001. “Sistema de Gestión de la Seguridad de la Información”. {En línea}. {05 Diciembre de 2017}.Disponible en http://www.gesconsultor.com/iso-27001.html

AGENCIA EFE. Hackers han realizado 5.500 ataques cibernéticos en 2017. En: El colombiano.com. Envigado: (2017), Disponible en http://www.elcolombiano.com/colombia/hackers-han-realizado-5-500-ataques-ciberneticos-en-2017-YD7126742

Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

FRANCO, Tovar. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. {En línea}. 2017. {5 Diciembre de 2017}. Disponible en http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. TECNOLOGÍA DE LA INFORMACIÓN.TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. Bogotá. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO. DIRECTRICES DE LA OCDE

PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD. Paris. Disponible en

http://www.oecd.org/internet/ieconomy/34912912.pdf

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. GUIA PARA LA IMPLEMENTACION DE LA SEGURIDAD DE LA INFORMACION. Bogotá. (06 de Noviembre de 2016). Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

NTC-ISO/IEC-27001. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). Bogotá. (22 de Marzo de 2006). Obtenido de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20

LINUX ADICTOS. “Herramientas de Kali Linux”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.linuxadictos.com/las-5-mejores-herramientas-encontraremos-kali-linux.html

VOUTSSÁS MÁRQUEZ, Juan. Preservación documental digital y seguridad informática. En: Investigación bibliotecológica, Vol. 24. No. 50. (Ene/Abr, 2010). p. 127-155.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

GUERRERO ERAZO, Henry Aldemar. LASSO GARCES, Lorena Alexandra & LEGARDA MUÑOZ, Paola Alexandra. IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S. Pasto. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3451/1/5203676.pdf

AGUILERA, Purificación. Seguridad informática. 1ª Ed. Madrid: Editex, 2010. p.9

ARÉVALO, Julio Alonso. Gestión de la Información, gestión de contenidos y conocimiento. En: MediCiego (2012). MediCiego. Vol.18. No. 1. (Nov, 2007); Disponible en http://www.bvs.sld.cu/revistas/mciego/alfin_2012/alfin_folder/2012%20Unidad%206/Bibliograf%EDa/Lect%20B%E1sicas/Lectura_basica_5.Gestion_de_la_informacion_gestion_de_contenidos_y_conocimiento.pdf

PONJUÁN DANTE, Gloria. Gestión de información. Dimensiones e implementación para el éxito organizacional. 1ª Ed. La Habana - Cuba: TREA, 2007.

UNIVERSIDAD NACIONAL DE LUJAN, Amenazas a la Seguridad de la Información, Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

FRANCO David, PEREA Jorge, y TOVAR Luis (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

MONSALVE Julián, APONTE Fredy y CHAVES David. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia), En: Revista Facultad de Ingeniería (Fac. Ing.), Vol. 23, No. 37 (Jul-Dic, 2014); pp. 65-72.

RAMOS RAMOS Jorge Luis. PRUEBAS DE PENETRACIÓN O PENT TEST, En: Revista de Información, Tecnología y Sociedad, No. 8 (Jun, 2013); pp. 31-33.

HERNÁNDEZ SAUCEDO, Ana Laura; MEJIA MIRANDA, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web, En: Revista electrónica de Computación, Informática Biomédica y Electrónica, Vol. 4 No. 15 (Feb, 2015).

Ministerio de las TIC – MINTIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Disponible en Internet:
https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

MOLINA MIRANDA, María Fernanda. PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL. Madrid. 2015, 89. Trabajo fin de master. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en:

http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

KALI LINUX. Nuestra distribución más avanzada de pruebas de penetración. Disponible en https://www.kali.org/

NMAP.org. (2017). Disponible en https://nmap.org/

Informa (2018). Directorio de empresas de Colombia. Disponible en https://www.informacion-empresas.co/Empresa_TALLER-INDUSTRIAL-ALKAN-SAS.html

FIRMA-E consultoría & desarrollo, Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad, Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

IANA, Agencia de Asignación de Números de Internet [en línea], [diciembre 2017]. Disponible en Internet: https://www.iana.org/

Snort. Sistemas de Detección de intrusos [en línea], diciembre2017]. Disponible en Internet: https://www.snort.org/

Soporte Técnico de Microsoft. Ms08-67 [en línea], [Abril 2018]. Disponible en Internet: https://support.microsoft.com/es-co/help/958644/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execu

12 ANEXOS

ANEXO 1. RESULTADOS DE LA EJECUCIÓN DE PRUEBAS

1. IDENTIFICACIÓN DE LA INFORMACIÓN PARA EL DESARROLLO DEL PROYECTO

Para el desarrollo del proyecto se utilizaron Inspección visual de estaciones de trabajo, reuniones, charlas, entrevistas a todo el personal involucrado en este proceso, siempre acompañados del ingeniero de sistemas responsable de la red con el fin de localizar las vulnerabilidades a que está expuesta la red.

En este proceso se identificó algunas políticas de seguridad:

1. Seguridad de información: Crean usuarios con su respectivo permiso y acceso a la aplicación asignada.

2. Seguridad de usuarios: Crean nombre de usuario con rol y perfil especifico rigiendo en el la política asignada y su contraseña que es personal e intransferible. Los usuarios son divididos en grupos llamados de consulta, administrador, desarrollador.

3. Tienen listado de usuarios con sus roles, permisos.

4. administración de contraseñas: Se tiene todo el conocimiento de usuarios y perfil conocido por el ingeniero de sistemas.

2. IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN QUE CONFORMAN LA RED DE DATOS DE LA EMPRESA

En Guadalajara de Buga se encuentra la principal, con oficina para el departamento de sistemas, encargada de mantener el sistema de red funcionando, en ella se identificaron los activos de información de la red de datos.

Terminal de usuario	Hardware
Base de datos	Software
Computador torre de escritorio	Hardware
Router	Red
Antivirus	Software
Modem	Hardware
Fuente de alimentación	Hardware
Programas	Software
Empleados	Personal

3. APLICACIONES DE SOFTWARE UTILIZADAS PARA EL ANALISIS DE LA RED DE DATOS

En estas pruebas de seguridad se utilizaron las siguientes aplicaciones:

Kali Linux: Sirve para evaluar la seguridad de las redes.

Nmap: Sirve para detectar puertos abiertos.

SqlMap: Sirve para obtener listas y registros de las bases de datos por medio de la inyección de SQL.

WireShark: Sirve para analizar los protocolos y el tráfico de la red de datos de información.

Ettercap: Sirve para interceptar o como sniffer de la red, aunque también es utilizado para auditorías en distintos tipos de redes. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS).

3.1. Pruebas de contraseña y nombre de usuario.

Contraseña invalida

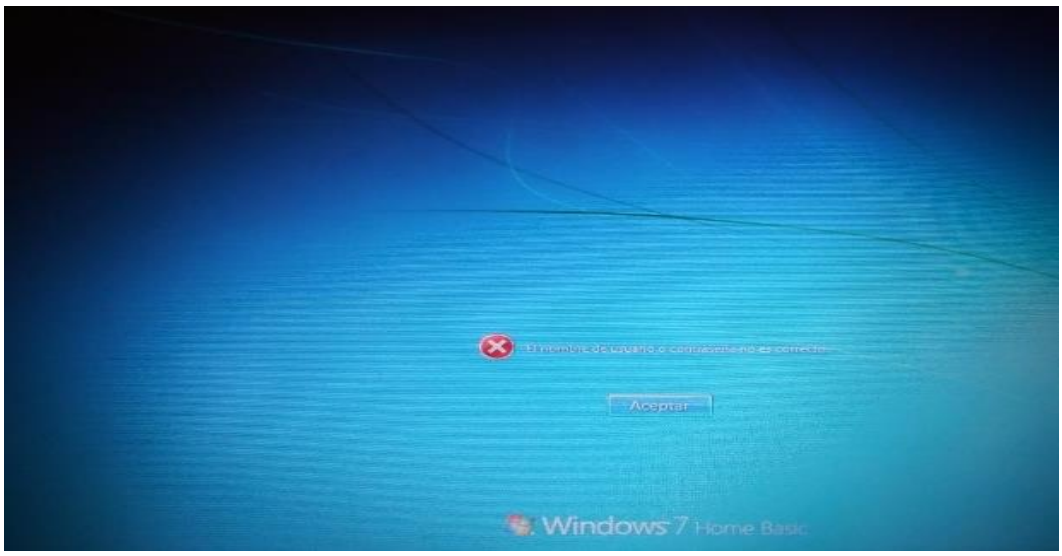
En las ilustraciones 1 y 2, se puede visualizar que al escribir la contraseña incorrecta la terminal no permite el acceso a los programas y aplicativos del sistema.

Ilustración 2. Contraseña valida

Fuente. Autor

La seguridad de la contraseña por ser de 8 dígitos alfanumérica es segura.

Ilustración 3. Acceso denegado



Fuente. Autor.

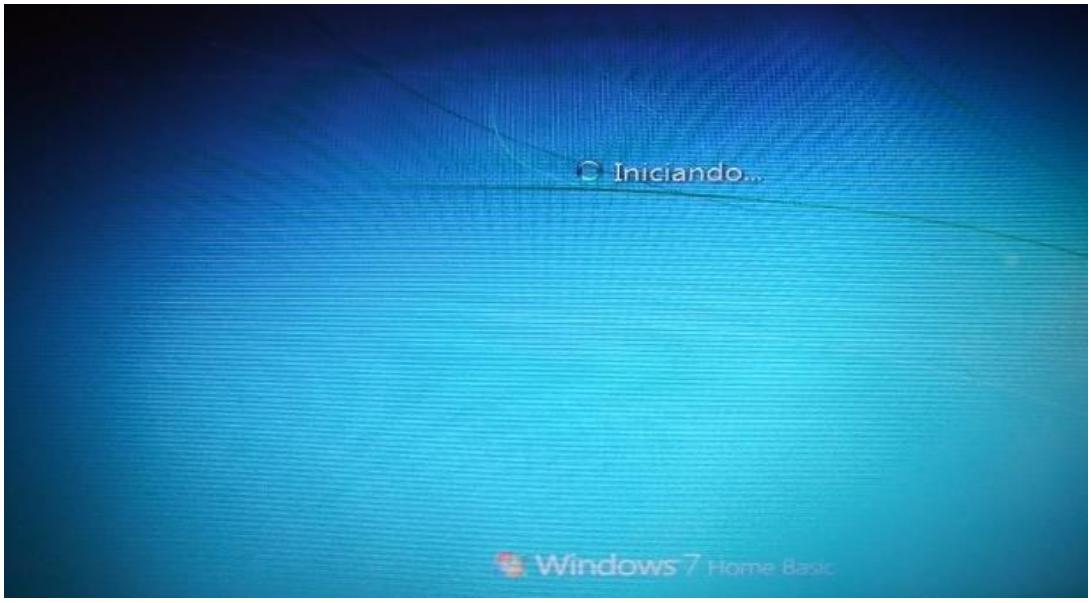
Contraseña valida

En las ilustraciones 3 y 4, se puede visualizar que al escribir la contraseña correcta la terminal permite el acceso a los programas y aplicativos del sistema.

Ilustración 4. Contraseña correcta

Fuente. Autor

Ilustración 5. Contraseña correcta



Fuente. Autor

Ilustración 6. Acceso total

Fuente. Autor

ANEXO 2. PUERTOS ABIERTOS

Tabla 18. Puertos abiertos

PUERTO	PROTOCOLO	DESCRIPCIÓN
21	Puerto de FTP	Usado para la descarga de archivos al equipo.
23	Puerto Telnet	Protocolo usado para comunicación.
25	Puerto SMTP	Usado por los clientes de email para enviar correo electrónico.
80	Puerto HTTP	Es el usado por los navegadores para cargar las páginas web.
110 y 995	Puertos POP3	Usados por los clientes de email para la recepción del correo.
119	Puerto NNTP	Servidor de noticias.
139	NetBIOS	Usado para compartir servicios compartidos de impresoras y/o archivos.
443	Puerto HTTPS	Usado para la carga segura de páginas web.
445	MSFT DS	Server Message Block.
531	Puerto IRC	Usado para servicios de chat.
1527	tlisrv	Puerto para Oracle y SQL.
1723	PPTP	Virtual prívate network (VPN). Puerto usado para conectar equipos por medio de Red Privada Virtual.
3306	MySQL	Puerto para Mysql (Bases de datos)
4661		Puertos usados para Conexiones Peer to Peer como Emule y otros.

Fuente. Autor

ANEXO 3. RANGO DE LOS PUERTOS SEGUNA AIANA (AGENCIA DE ASIGNACION DE NUMEROS INTERNET)

Tabla 19. Rango puertos asignados por internet

Categoría	Descripción
0 - 1023	Se denominan puertos reservados para usos específicos que se encuentran reglamentados, el sistema operativo los abre para permitir su empleo por diversas aplicaciones mediante los llamados protocolos, por ejemplo: HTTP, FTP, TELNET, IRC, POP3, etc.
1024 – 49151	Se denomina "Registrados" estos puertos pueden ser usados por cualquier aplicación.
49152 – 65535	Se denominan "Dinámicos o privados", estos puertos los usa el sistema operativo cuando una aplicación tiene que conectarse a un servidor y se le realiza la solicitud de un puerto.

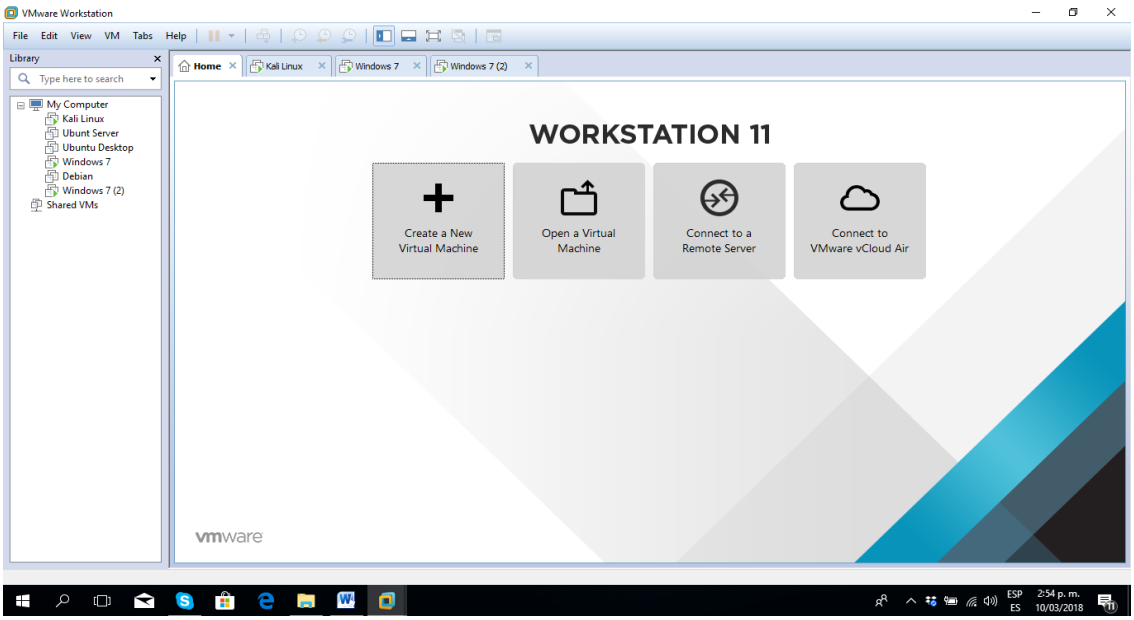
Fuente. Autor

ANEXO 4. INSTALACIÓN Y CONFIGURACIÓN DEL AMBIENTE DE TRABAJO

4.1. INSTALACIÓN DE LA APLICACIÓN VMWARE

Esta aplicación se descarga de la página oficial y se instala en el sistema operativo Windows. Link https://www.vmware.com/co/download/open_source.html

Ilustración 7. VMWare instalado

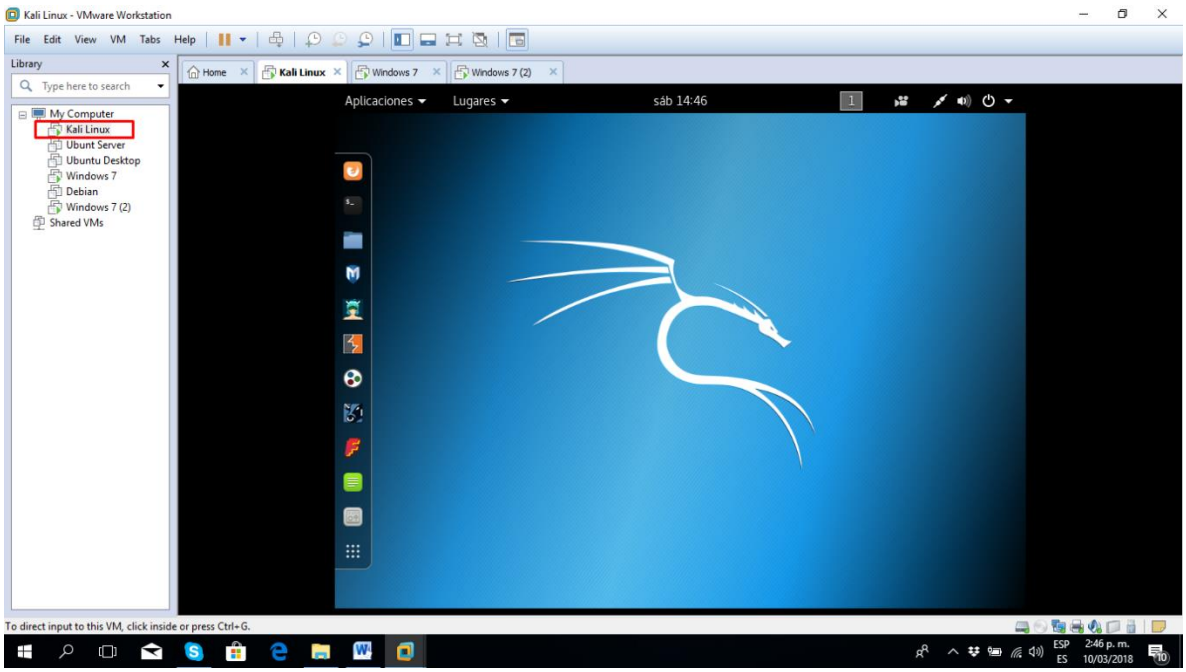


Fuente. Autor

4.2. INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA OPERATIVO KALI LINUX

Se instala el Kali linux descargado de la página oficial https://www.kali.org/ en el sistema operativo virtual VMWare.

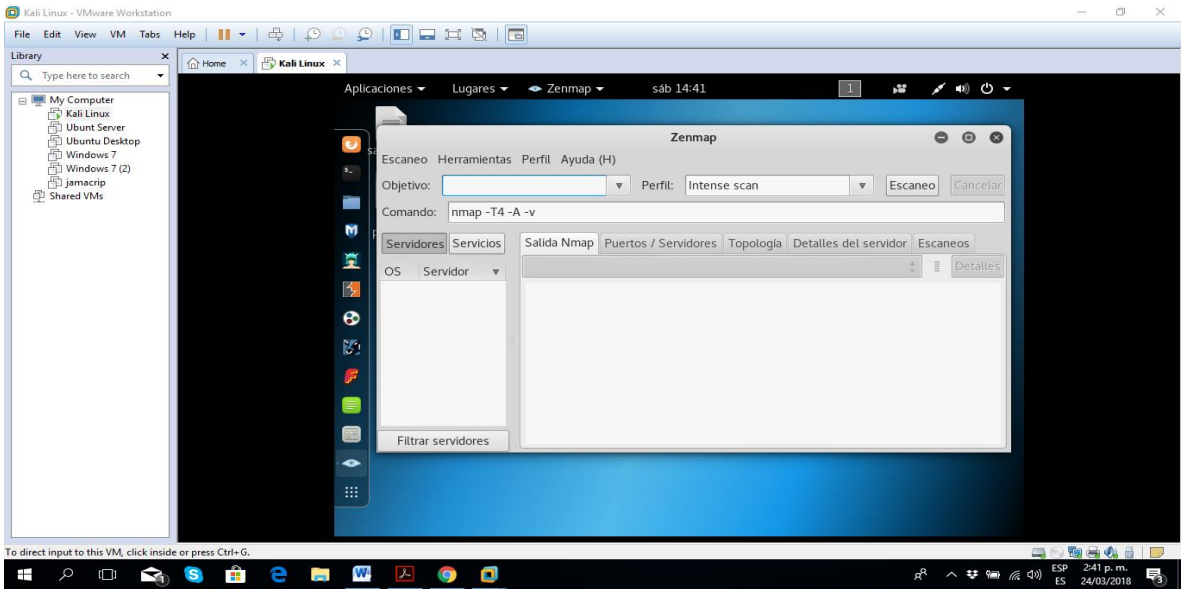
Ilustración 8. Kali Linux instalado



Fuente. Autor

4.3. VERIFICACION DE NMAP EN KALI LINUX

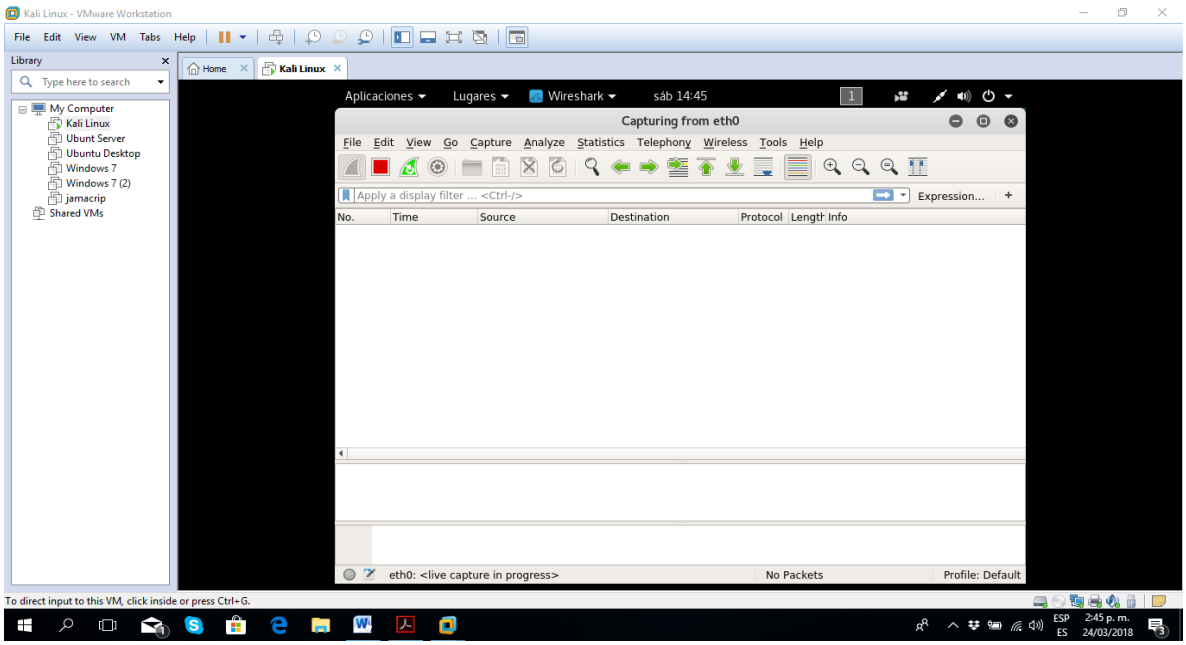
Ilustración 9. Nmap



Fuente. Autor

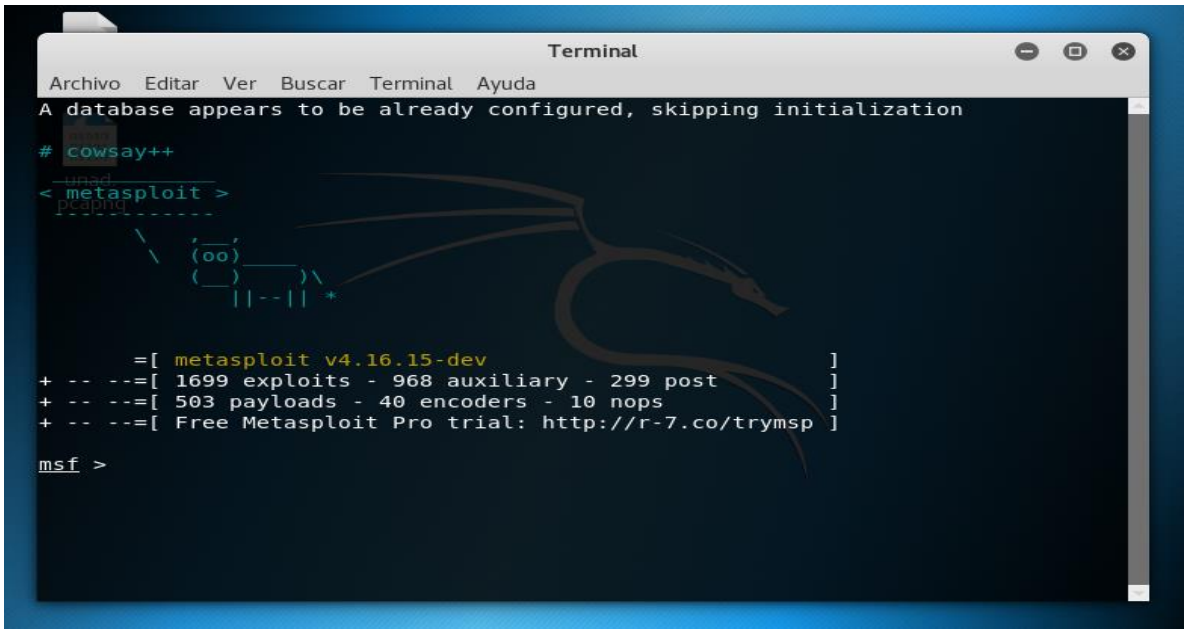
4.4. VERIFICACION DE WIRESHARK EN KALI LINUX

Ilustración 10. Wireshark



Fuente. Autor

Ilustración 11. Metasploit

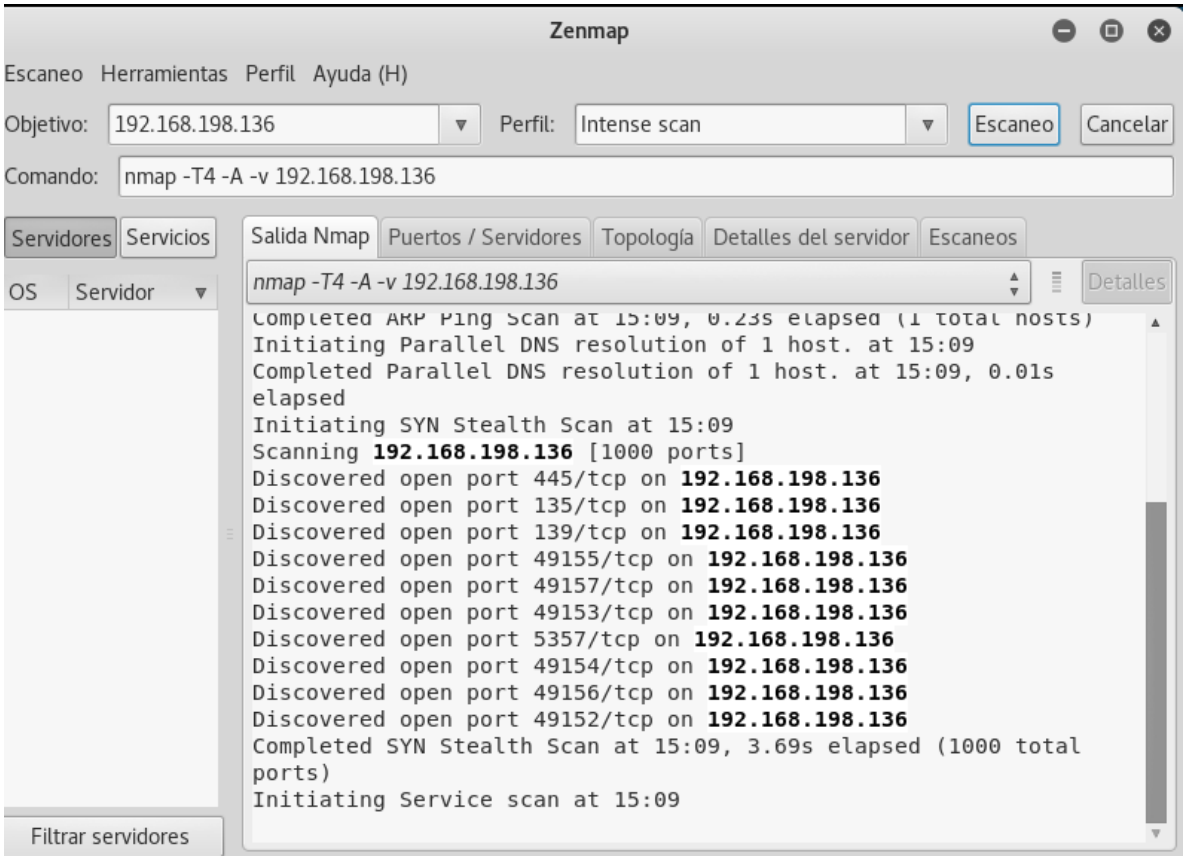


Fuente. Autor

ANEXO 5. PRUEBAS REALIZADAS CON HERRAMIENTAS DE PENTESTING

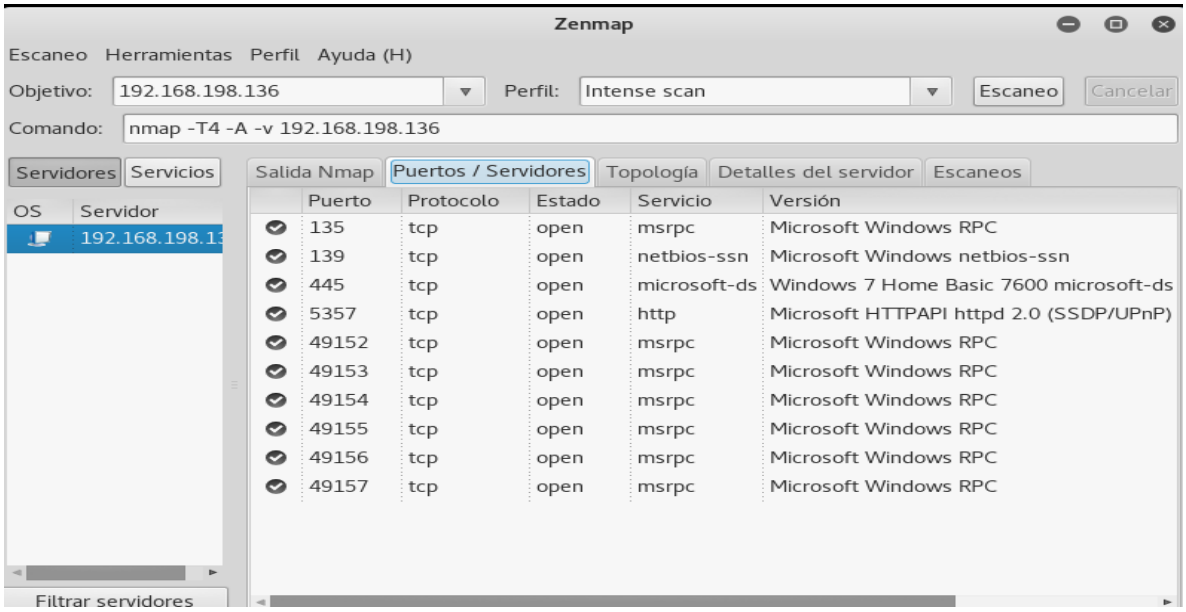
Utilizando la herramienta de Pentesting Zenmap la cual sirve para detectar vulnerabilidades en los sistemas, evaluando la red y determinar posibles vulnerabilidades. Usando la herramienta de Kali Linux con el programa NMAP, para escanear los puertos que están abiertos, usando el comando: Nmap -sV -T4 -Pn “IP maquina a vulnerar”. En nuestro caso Nmap -sV -T4 -Pn 192.168.198.136.

Ilustración 12. Comando escaneo puertos abiertos



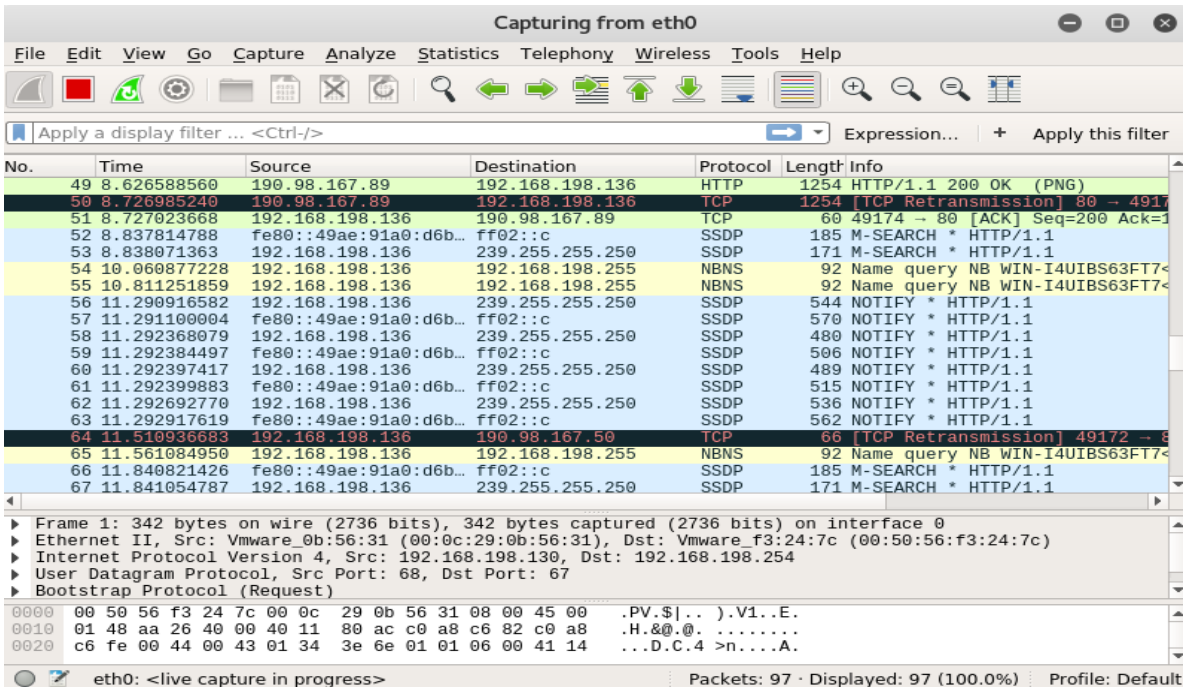
Autor. Fuente

Ilustración 13. Escaneo de puertos y servicios



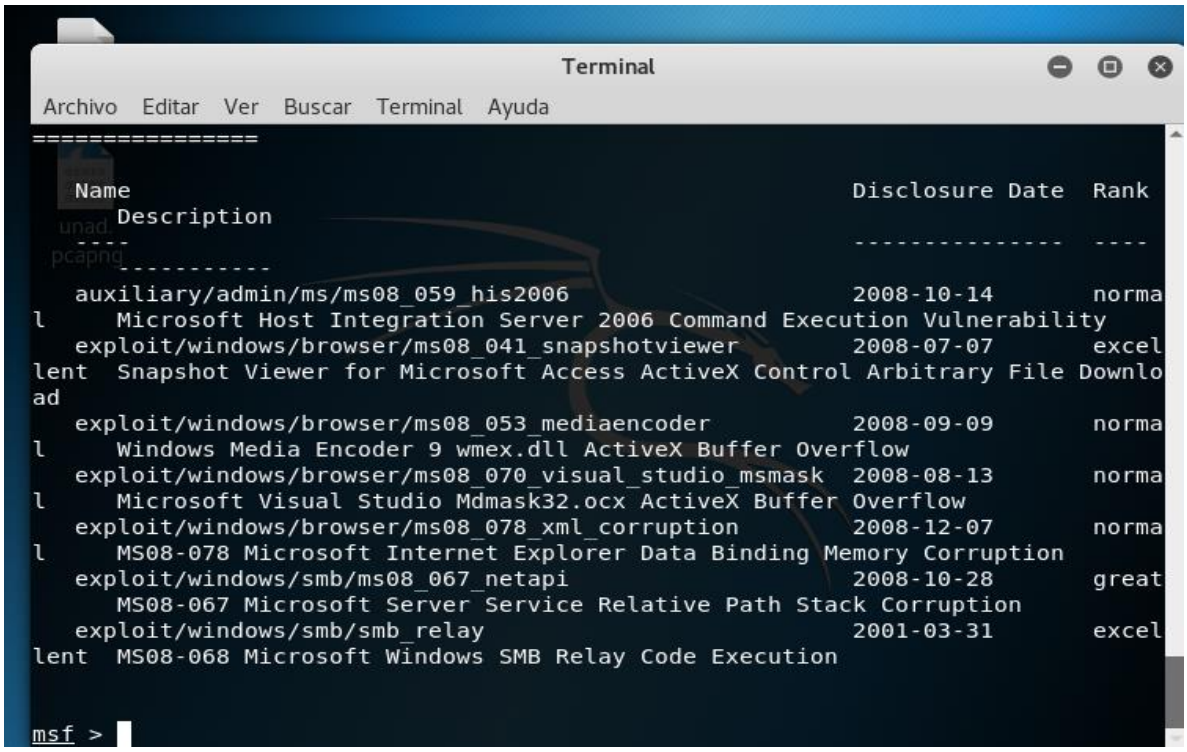
Fuente. Autor

Ilustración 14. Scaneo de la red con Wireshark



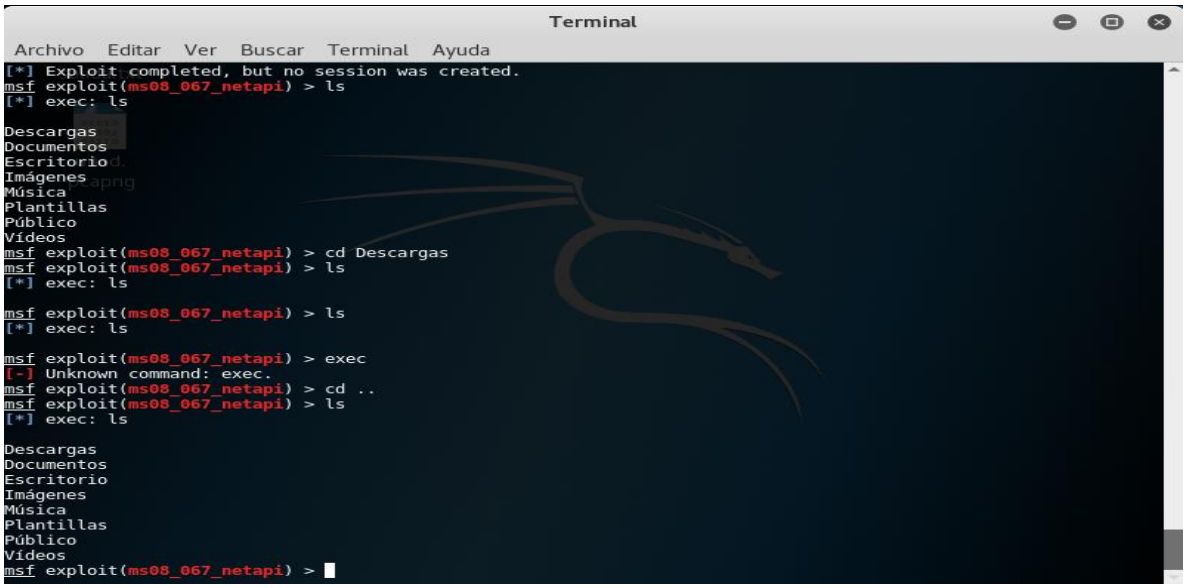
Fuente. Autor

Ilustración 15. Explotar las vulnerabilidades con metasploit, vulnerabilidad ms08



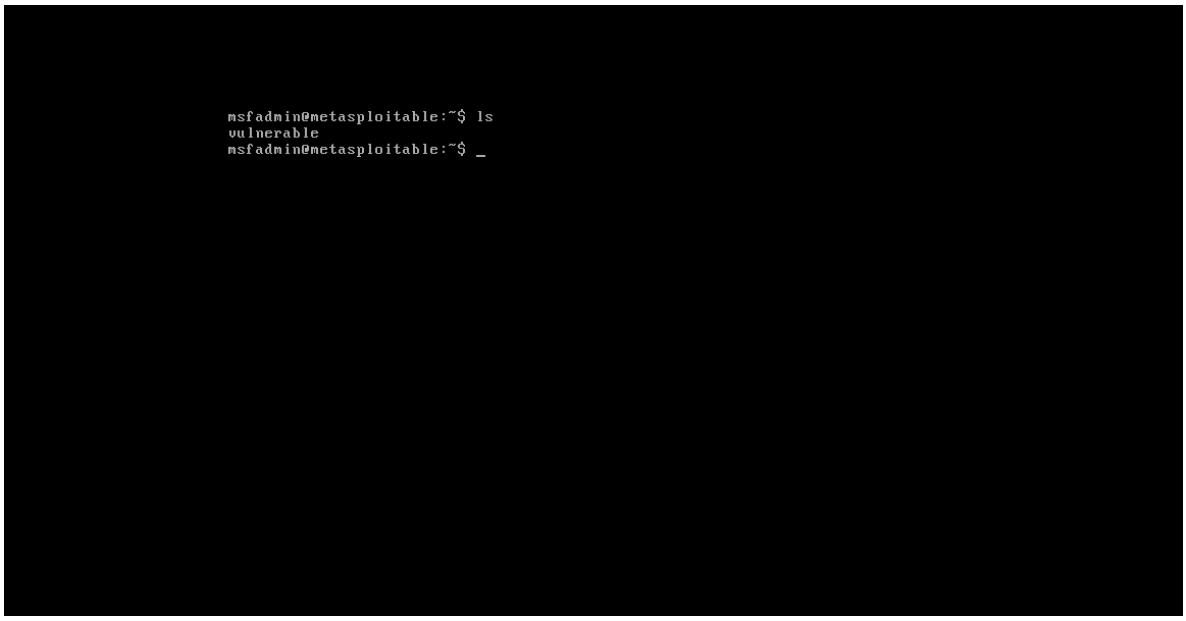
Fuente. Autor

Ilustración 16. Entrada al equipo vulnerable de Sistemas



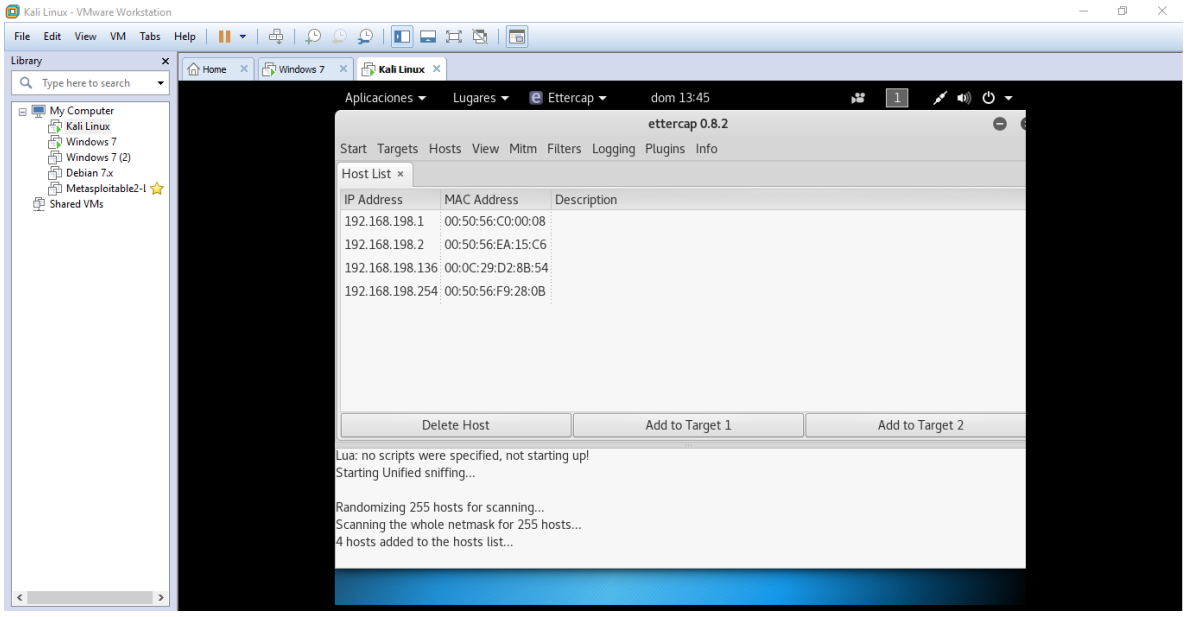
Fuente. Autor

Ilustración 17. Equipo vulnerables



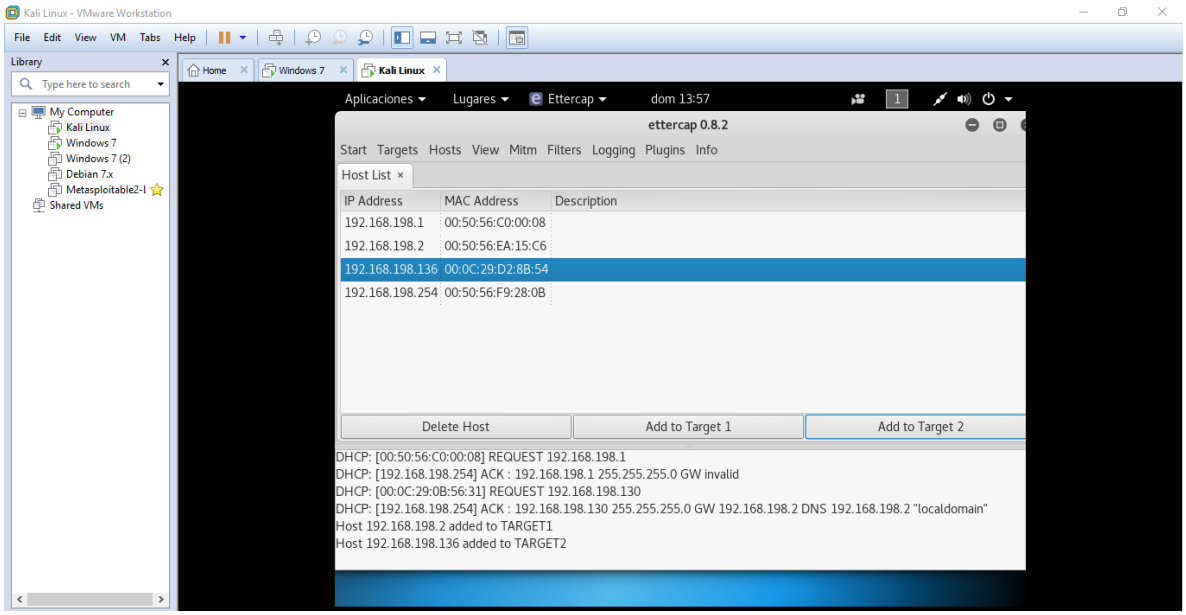
Fuente. Autor

Ilustración 18.Prueba de vulnerabilidad MITM (Man in the Middle) con la herramienta Ettercap



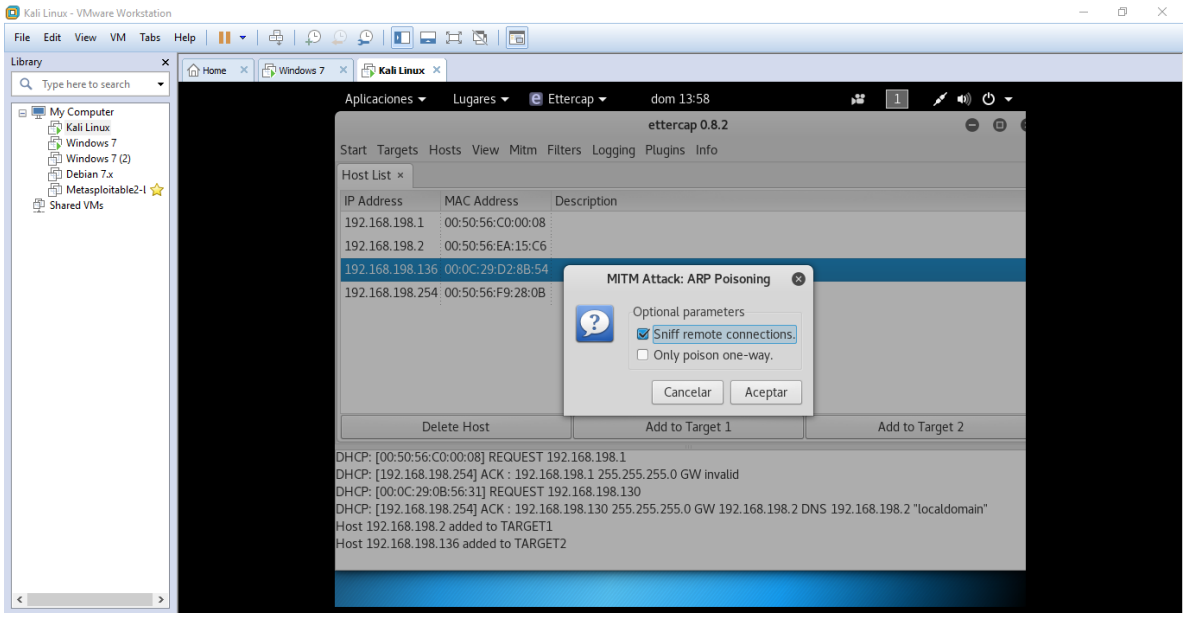
Fuente. Autor

Ilustración 19. Asignación de los Target en Ettercap



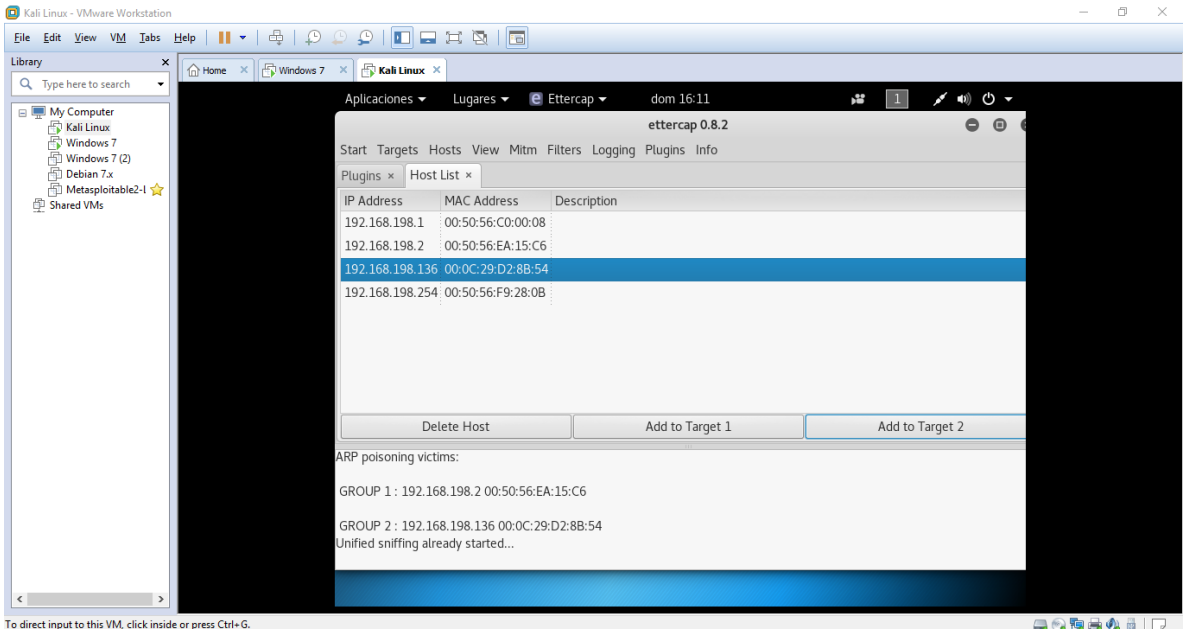
Fuente. Autor

Ilustración 20. Envenenamiento del Arp con Ettercap



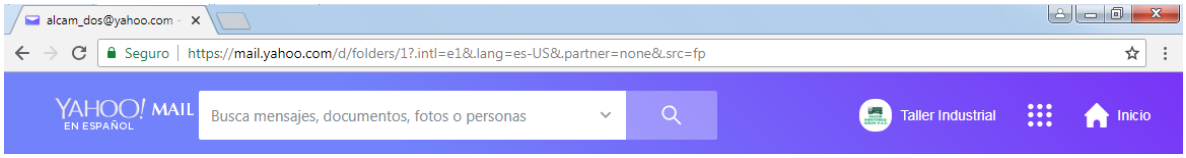
Fuente. Autor

Ilustración 21. Inicio del Sniffin con el plugin Remote_Browser



Fuente. Autor

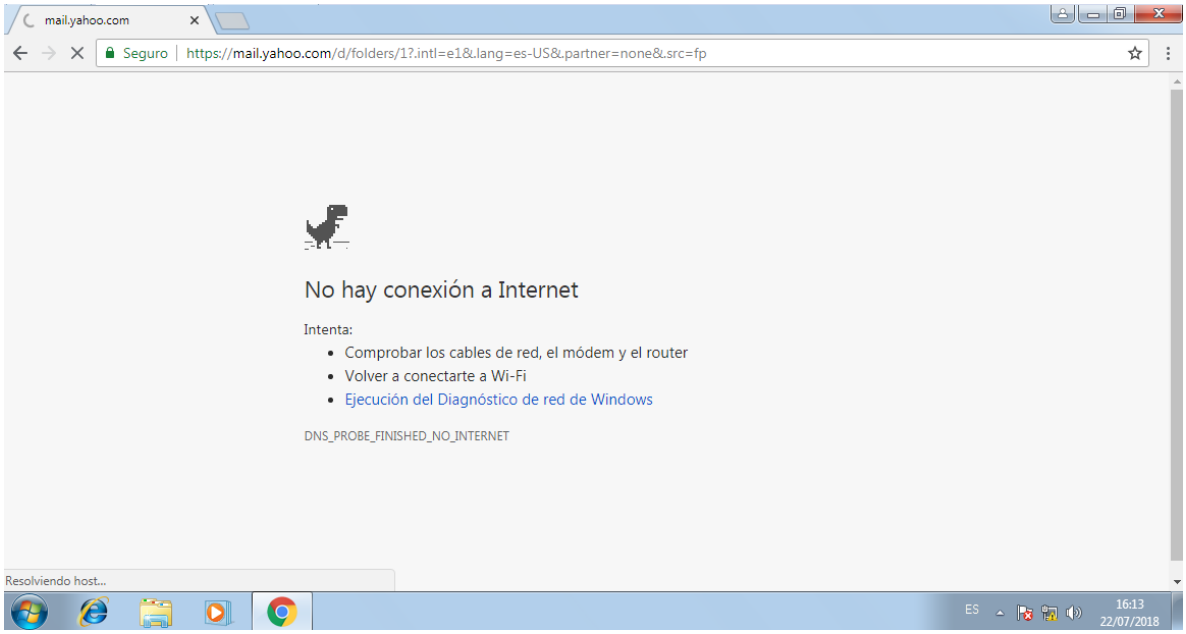
Ilustración 22. Equipo del Taller Industrial Alkan navegando normalmente en su correo institucional



Fuente. Autor

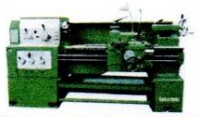
Debido a que el router está bien configurado en su seguridad con el firewall, este tipo de prueba arrojo excelentes resultados de protección ante este ataque demostrando que la empresa cuenta con un buen router configurado adecuadamente.

Ilustración 23. Fallo del internet en el equipo del Taller Industrial Alkan por el envenenamiento del ARP



Fuente. Autor

ANEXO 6. CARTA AUTORIZACION DE LA EMPRESA PARA EL DESARROLLO DEL PROYECTO



TALLER INDUSTRIAL ALKAN S.A.S.

Mantenimiento y Reparación Especializado de Maquinaria y Equipo Industrial

Teléfono Fijo 227 5940 – Celular: 317 8597112-3127246772 - E-mail: alcam_uno@yahoo.com
Taller: Carrera 17 # 16-30 Guadalajara de Buga (Valle)
NIT 900.882.264-6

Guadalajara de Buga, Febrero 15 del 2018

SEÑORES
UNAD
PALMIRA

Damos a conocer a ustedes que a partir de la fecha autorizamos a ADRIAN PASTRANA FRANCO Y JAVIER MARMOLEJO SERRANO para que inicien el proyecto en las REDES DE INFORMACION en Nuestra empresa donde se buscaran vulnerabilidades. Dicho proyecto tendrá un término de duración de cuatro (4) meses.

ATENTAMENTE

TALLER INDUSTRIAL ALKAN S.A.S. NIT 900.882.264-6

Gerardo A Garcia G

GERARDO ALONSO GARCIA GARCIA
Representante legal.

NOTA: Se informa que toda la información que se manejara es de uso exclusivo de la empresa Y la Universidad.

ANEXO 7. RESUMEN ANALÍTICO ESPECIALIZADO – RAE

1. Información General	
Tema	Análisis y evaluación de vulnerabilidades en la seguridad informática de la empresa Taller Industrial Alkan S.A.S
Titulo	PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA TALLER INDUSTRIAL ALKAN S.A.S DE LA CIUDAD GUADALAJARA DE BUGA, VALLE PARA IDENTIFICAR VULNERABILIDADES
Tipo de proyecto	Proyecto aplicado
Autor (es)	Ingeniero Javier Marmolejo Serrano – Ingeniero Adrian Pastrana Franco
Director	Mg. Yina Alexandra González Sanabria
Fuente Bibliográfica	SANTANA, Carlos. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. {En línea}. 2012. {7 Septiembre de 2012}. Disponible en https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo EcuRed. Kali Linux. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://www.ecured.cu/Kali_linux NORMA ISO 27001. “Sistema de Gestión de la Seguridad de la Información”. {En línea}. {05 Diciembre de 2017}.Disponible en http://www.gesconsultor.com/iso-27001.html AGENCIA EFE. Hackers han realizado 5.500 ataques

cibernéticos en 2017. En: El colombiano.com. Envigado: (2017), Disponible en http://www.elcolombiano.com/colombia/hackers-han-realizado-5-500-ataques-ciberneticos-en-2017-YD7126742

Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. 2018. {20 Mayo de 2018}. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WwGBZUiFPIU

FRANCO, Tovar. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. {En línea}. 2017. {5 Diciembre de 2017}. Disponible en http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. TECNOLOGÍA DE LA INFORMACIÓN.TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. Bogotá. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO. DIRECTRICES DE LA OCDE

PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD. Paris. Disponible en

http://www.oecd.org/internet/ieconomy/34912912.pdf

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. GUIA PARA LA IMPLEMENTACION DE LA SEGURIDAD DE LA INFORMACION. Bogotá. (06 de Noviembre de 2016). Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

NTC-ISO/IEC-27001. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). Bogotá. (22 de Marzo de 2006). Obtenido de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20

LINUX ADICTOS. “Herramientas de Kali Linux”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.linuxadictos.com/las-5-mejores-herramientas-encontraremos-kali-linux.html

VOUTSSÁS MÁRQUEZ, Juan. Preservación documental digital y seguridad informática. En: Investigación bibliotecológica, Vol. 24. No. 50. (Ene/Abr, 2010). p. 127-155.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

GUERRERO ERAZO, Henry Aldemar. LASSO GARCES, Lorena Alexandra & LEGARDA MUÑOZ, Paola Alexandra. IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN

DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S. Pasto. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3451/1/5203676.pdf

AGUILERA, Purificación. Seguridad informática. 1ª Ed. Madrid: Editex, 2010. p.9

ARÉVALO, Julio Alonso. Gestión de la Información, gestión de contenidos y conocimiento. En: MediCiego (2012). MediCiego. Vol.18. No. 1. (Nov, 2007); Disponible en http://www.bvs.sld.cu/revistas/mciego/alfin_2012/alfin_folder/2012%20Unidad%206/Bibliograf%EDa/Lect%20B%E1sicas/Lectura_basica_5.Gestion_de_la_informacion_gestion_de_contenidos_y_conocimiento.pdf

PONJUÁN DANTE, Gloria. Gestión de información. Dimensiones e implementación para el éxito organizacional. 1ª Ed. La Habana - Cuba: TREA, 2007.

UNIVERSIDAD NACIONAL DE LUJAN, Amenazas a la Seguridad de la Información, Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

FRANCO David, PEREA Jorge, y TOVAR Luis (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003

MONSALVE Julián, APONTE Fredy y CHAVES David. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia), En: Revista

Facultad de Ingeniería (Fac. Ing.), Vol. 23, No. 37 (Jul-Dic, 2014); pp. 65-72.

RAMOS RAMOS Jorge Luis. PRUEBAS DE PENETRACIÓN O PENT TEST, En: Revista de Información, Tecnología y Sociedad, No. 8 (Jun, 2013); pp. 31-33.

HERNÁNDEZ SAUCEDO, Ana Laura; MEJIA MIRANDA, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web, En: Revista electrónica de Computación, Informática Biomédica y Electrónica, Vol. 4 No. 15 (Feb, 2015).

MOLINA MIRANDA, María Fernanda. PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL. Madrid. 2015, 89. Trabajo fin de master. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en:

http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

KALI LINUX. Nuestra distribución más avanzada de pruebas de penetración. Disponible en https://www.kali.org/

NMAP.org. (2017). Disponible en https://nmap.org/

Informa (2018). Directorio de empresas de Colombia. Disponible en

https://www.informacion-empresas.co/Empresa_TALLER-INDUSTRIAL-ALKAN-SAS.html

	FIRMA-E consultoría & desarrollo, Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad, Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/ IANA, Agencia de Asignación de Números de Internet [en línea], [diciembre 2017]. Disponible en Internet: https://www.iana.org/ Snort. Sistemas de Detección de intrusos [en línea], diciembre2017]. Disponible en Internet: https://www.snort.org/
Año	2.018
Resumen	El presente proyecto aplicado consiste en hallar vulnerabilidades a la empresa Taller Industrial Alkan S.A.S por medio de las etapas que consisten en el levantamiento de información de activos informáticos de la empresa, aplicar pruebas de pentesting a la red, valorar las vulnerabilidades encontradas según los riesgos detectados en las pruebas de testeo de red y su efecto en el sistema de información y plantear estrategias de reducción de los riesgos encontrados para evitar y reforzar la seguridad de la información. Para lograr estas etapas se usa la norma ISO IEC 27001 (2006), la cual da una variedad de controles para evaluar los riesgos asociados a la seguridad de la información, el modelo Magerit que permite analizar y gestionar los riesgos de sus sistema, Aplicar pruebas de penetración a la red de datos empleando la metodología del ethical hacking con la herramienta Kali Linux para diagnosticar las vulnerabilidades de seguridad de la información y realizar un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e

	instrumentos seleccionados y las pruebas de penetración para plantear estrategias de reducción de los riesgos encontrados para evitar y reforzar la seguridad de la información.
Palabras Claves	Vulnerabilidades, Seguridad, Seguridad informática, Control de acceso, Sistema de gestión de información, Pentest.
Contenidos	Hoy en día ninguna organización está exenta de esta clase de vulnerabilidades, amenazas o ataques, que deben ser detectados a tiempo para así diseñar una serie de controles que las contrarresten, para lograrlo se han creado diferentes normas, entre las cuales existe la norma ISO/IEC 27001 que proporcionan un marco de gestión de la seguridad de la información que puede adaptarse por cualquier organización pública o privada, grande o pequeña, en el proyecto se hará uso de las normas ISO 27001 de activos de información de controles de seguridad. Impulsados en lo anterior se presenta un proyecto enfocado en un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 para la unidad de Informática de la empresa Taller Industrial Alkan S.A.S, ya que la información es un factor clave de éxito y por lo tanto su eficiente administración garantiza altos estándares de calidad y productividad. El desarrollo de este proyecto implicó la definición de los activos que necesitan protegerse, junto con los riesgos, vulnerabilidades, amenazas y controles existentes para cada uno de ellos. Una vez hecho esto, se continuó con la definición nuevos controles necesarios para cada uno de los activos, y como resultado un sistema de gestión de seguridad de la información (SGSI), que mejor se ajuste a las necesidades actuales y que permita gestionar de manera eficiente la información para la Unidad, asegurando la integridad, confidencialidad y disponibilidad de la misma y con esto la mejora continua de la empresa.
2. Descripción del Problema de Investigación	
¿Las pruebas de penetración a la red de la empresa solucionarían los problemas	

de vulnerabilidad en la seguridad de la información de la empresa taller Alkan S.A.S?

La empresa talleres Alkan S.A.S es una empresa con buena trayectoria, con un excelente crecimiento debido a factores de los excelentes servicios que ofrecen en el área metalmecánica, así como las excelentes estrategias de servicio de alto standing. Para su funcionamiento se hace uso de las redes sociales que han gozado de excelente aceptación y por lo tanto se hace indispensable tener una buena protección en la seguridad informática que permita salvaguardar la comunicación e información. Hasta la fecha esta empresa no cuenta con la seguridad informática adecuada y ha presentado problemas como la desaparición de alguna información sobre datos de clientes, bloqueo de archivos, perdidas de conectividad sin explicación alguna, duplicación de la información y derivación de información comercial no propia de la empresa por parte externa.

El sistema de gestión de la seguridad en la información está orientado en proteger el sistema de información utilizando protocolos, normas y herramientas para disminuir daños en el software, bases de datos y toda la información empresarial. En el caso de la empresa se beneficiarían de este proyecto en cuanto la conservación de la integridad, disponibilidad, confidencialidad, autenticidad de la información, en el desarrollo y crecimiento de sus metas, para asegurar los sistemas informáticos y evitar pérdidas de información lo cual influye en el cumplimiento de la misión empresarial, de igual manera este beneficio causara un impacto positivo en el sector de servicios metalmecánicos que es uno de los campos económicos a explotar en la región del Valle del Cauca.

La importancia de la seguridad informática

De acuerdo a la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001[5], las instituciones públicas y empresas privadas se ven obligadas a revisar el uso de

los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas. Debido a esto es primordial que el sistema de la información de la empresa taller industrial Alkan S.A.S que contiene información comercial, reportes, correspondencia interna y externa, sea un sistema vital y seguro para la empresa la cual se obliga a estar protegida.

Al efectuar un rastreo de vulnerabilidades al sistema de la información, permitirá evaluar sus condiciones de seguridad lo cual facilitara el planteamiento de un plan de reducción de vulnerabilidades que a futuro mantenga un sistema de información confiable, íntegro y disponible que además evitará los riesgos a los cuales estaría comprometido reduciendo el impacto negativo en el funcionamiento de la empresa.

3. Objetivos

OBJETIVO GENERAL

Realizar pruebas de penetración a la infraestructura tecnológica de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle para identificar vulnerabilidades.

OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento de los activos de información de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle mediante la metodología Magerit.

- Aplicar pruebas de penetración a la red de datos empleando la metodología del ethical hacking con la herramienta Kali Linux para diagnosticar las vulnerabilidades de seguridad de la información de la empresa Talleres Alkan S.A.S de la ciudad Guadalajara de Buga, Valle.

- Valorar las vulnerabilidades encontradas según los riesgos detectados en las pruebas de testeo de red y su efecto en el sistema de información.

- Plantear estrategias de reducción de los riesgos encontrados para evitar y reforzar la seguridad de la información.

4. Referentes Teóricos

LINUX ADICTOS. “Herramientas de Kali Linux”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.linuxadictos.com/las-5-mejores-herramientas-encontraremos-kali-linux.html

VOUTSSÁS MÁRQUEZ, Juan.Preservación documental digital y seguridad informática. En: Investigación bibliotecológica, Vol. 24. No. 50. (Ene/Abr, 2010). p. 127-155.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En linea}. {5 de Diciembre de 2017}. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

GUERRERO ERAZO, Henry Aldemar. LASSO GARCES, Lorena Alexandra & LEGARDA MUÑOZ, Paola Alexandra. IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S. Pasto. Disponible en http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3451/1/5203676.pdf

AGUILERA, Purificación. Seguridad informática. 1ª Ed. Madrid: Editex, 2010. p.9

ARÉVALO, Julio Alonso. Gestión de la Información, gestión de contenidos y conocimiento. En: MediCiego (2012). MediCiego. Vol.18. No. 1. (Nov, 2007); Disponible en http://www.bvs.sld.cu/revistas/mciego/alfin_2012/alfin_folder/2012%20Unidad%206/Bibliograf%EDa/Lect%20B%E1sicas/Lectura_basica_5.Gestion_de_la_informacion_gestion_de_contenidos_y_conocimiento.pdf

PONJUÁN DANTE, Gloria. Gestión de información. Dimensiones e implementación para el éxito

organizacional. 1ª Ed. La Habana - Cuba: TREA, 2007.

5. Referentes Teóricos y Conceptuales

RAMOS RAMOS Jorge Luis. PRUEBAS DE PENETRACIÓN O PENT TEST, En: Revista de Información, Tecnología y Sociedad, No. 8 (Jun, 2013); pp. 31-33.

UNIVERSIDAD NACIONAL DE LUJAN, Amenazas a la Seguridad de la Información, Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

VOUTSSÁS MÁRQUEZ, Juan. Preservación documental digital y seguridad informática. En: Investigación bibliotecológica, Vol. 24. No. 50. (Ene/Abr, 2010). p. 127-155.

NORMA ISO 27001. “Sistema de Gestión de la Seguridad de la Información”. {En línea}. {05 Diciembre de 2017}.Disponible en http://www.gesconsultor.com/iso-27001.html

6. Resultados y Conclusiones

La red de la empresa Taller industrial Alkan S.A.S., no presenta ningún grado de complejidad para la administración y control de seguridad informática. A continuación, se presentarán las vulnerabilidades y recomendaciones que se le sugieren a la empresa para mejorar su seguridad en sus sistemas operativos y base de datos.

ADMINISTRATIVAS Y PERSONAL DE LA EMPRESA

Concientizar a los empleados de la empresa de la importancia que tiene la manipulación y confidencialidad de la información: Los funcionarios y empleados adquieren las responsabilidades y cuidados que se deben tener al manipular información confidencial de la empresa.

Todas las claves y privilegios que tienen los empleados de la empresa deben ser bloqueados a la hora que se termine el contrato de forma definitiva: En caso que el contrato termine en malos términos se debe impedir que el afectado despedido manipule la información.

Prohibir cualquier actividad de personal no autorizado en las áreas donde hay información y acceso a los equipos de cómputo: Se evitará daños en los equipos ya sea por derramamiento de líquidos o comida sobre ellos provocando la pérdida del equipo y de la información, además se evitará que personal no autorizado pueda acceder a la información de los usuarios.

Los empleados de la organización que ejercen funciones en los sistemas de información deberán ser capacitados periódicamente en materia de seguridad: El departamento de seguridad informática deberá difundir las políticas de seguridad implementadas por la empresa a todos los empleados en general.

Los usuarios de la empresa que tienen correo electrónico deberán conocer la importancia del uso del mismo, ya que, si no le damos un buen uso, se puede ser víctima de virus por descargas de archivos adjuntos: Los empleados deberán tomar conciencia del uso del correo electrónico, del riesgo a que están expuestos por el mal uso del mismo, solo se deberá utilizar para intercambiar información exclusiva de la empresa.

Es necesario que los empleados tengan claro los aspectos de integridad, disponibilidad y confiabilidad de los bienes y servicios de la entidad: Los empleados deberán adquirir el compromiso al momento de ser contratados de proteger y salvaguardar los activos informáticos, ya que es lo más valiosos que posee la organización y así se evitaran fugas de información.

BASE DE DATOS

Los resultados de las pruebas en la base de datos se identificaron las siguientes vulnerabilidades:

Algunos usuarios cuentan con políticas de contraseñas débiles, permite asignar contraseñas iguales al nombre de usuario fáciles de identificar, no cuenta con la longitud mínima de caracteres, para la construcción de la contraseña, no cuenta con criterios de asignación de caracteres especiales como condición obligatoria: Se recomienda establecer políticas más fuertes en la definición de contraseñas, contar con una longitud mínima, no asignar el mismo nombre de usuario a la clave y asignar un mínimo de caracteres especiales.

Usuarios en desuso: Se requerirá contar con tareas periódicas de monitoreo de la base de datos para identificar usuarios en desuso.

La información contenida en las bases de datos deberá ser usada únicamente para asuntos relacionados con actividades de la empresa: Los funcionarios y empleados deben dar buen uso a la información de las bases de datos y no utilizarla para su beneficio personal que no tiene nada que ver con la actividad de la empresa.

Todos los datos de gran importancia deberán ser respaldados y almacenados en un lugar seguro: El departamento de sistemas deberá estar pendiente de realizar copias de respaldo de la información más importante de la empresa, ya que de esta forma se protegerá la información y en caso de desastre se pueda recuperar.

La información contenida en las bases de datos solo la podrá utilizar y modificar el personal autorizado: Se deberá crear una política de control de acceso la cual debe ser gestionada por el administrador de base de datos.

Incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas: Actualizar las bases de datos, de esta forma la empresa contara con un historial de acceso a las bases de datos de los empleados en caso de un uso inadecuado de la información.

Implementar una política que administre y controle la eliminación de información de la base de datos que ya no sea necesaria: La base de datos no se recargará con información innecesaria y serán más rápidas las consultas.

INFRAESTRUCTURA Y RED

Socializar los procedimientos de prevención y mitigación de los riesgos informáticos: Difundir las políticas de riesgos tanto a las directivas como a los empleados de las diferentes áreas de la empresa, para prevenir futuros desastre en la red que puedan conllevar a la perdida en la información por culpa de ignorancia o desconocimiento de las políticas de seguridad informática implementada por la organización.

Cumplir con todas las políticas de seguridad establecidas por la organización: El departamento de seguridad informática está encargado, de que todos los empleados cumplan con las políticas de seguridad implementadas, para evitar riesgos informáticos, que puedan ocasionar daño a la red y fuga de su

información.

Actualizar el cronograma de mantenimiento de equipos preventivo y correctivo: La empresa deberá realizar un cronograma de mantenimiento periódico a los equipos, así se evitará futuros daños en los computadores y la red será más eficiente.

Se cuenta con un antivirus que no realiza una buena protección a los equipos, en ocasiones se pierde información por la existencia de código malicioso: La empresa deberá establecer un plan de protección del registro, establecer procedimientos de detención, prevención y corrección de software malicioso (Virus, troyanos, spyware, etc.), actualizando el sistema operacional y el antivirus periódicamente.

Mejorar la seguridad física, el ingreso de personal no autorizado: La empresa deberá hacer cumplir la política de control de acceso a las instalaciones, definir el perímetro de seguridad física, establecer mecanismos de protección contra amenazas externas y personal no autorizado en las diferentes áreas de la entidad.

Los equipos que no estén en uso deberán ser almacenados en un lugar seguro donde se restrinja el acceso al personal no autorizado: Se deberán destruir los equipos almacenados y que ya no son útiles, para evitar la pérdida o sustracción de la información que pueda ocasionar daño a la entidad.

Los equipos de cómputo serán asignados a un responsable para evitar el uso inadecuado del mismo: Así se mejorará la administración y mantenimiento de los

recursos informáticos de la organización.

El área de sistemas es la encargada de realizar los diferentes mantenimientos preventivo y correctivo de los quipos de cómputo: Para evitar deterioro de los equipos y una mala manipulación por personal no calificado.

Se deberá establecer controles de acceso en áreas donde se ubican los servidores y equipos de comunicación de la empresa: De esta forma se llevará un control de quien y a qué hora ingresa el personal autorizado a estas áreas.

Las contraseñas usadas para la configuración de equipos de red y telecomunicaciones deberán estar basadas en un estándar que defina aspectos como: estructura, tiempo de validez y reusabilidad: La utilización de contraseñas fuertes y difíciles de descifrar evitara el acceso no autorizado de personal a los equipos y a la información confidencial de la empresa.

El personal que realiza trabajos de configuración de los dispositivos de red deberá poseer una certificación que avale sus capacidades: El personal que manipule, configure y repare los equipos deberán estar calificados debidamente para que no comprometan la seguridad de la red.

Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red, debidamente codificados e identificados: Facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de Red.

Los puertos que no estén en uso deberán ser bloqueados adecuadamente: De

esta forma se evitarán accesos internos y externos de personal no autorizado a la red que puedan ocasionar daños y la manipulación de la información.

El acceso a Internet será restringido, solo para realizar labores propias de la empresa: Se deberán de bloquear algunas páginas de internet que no son necesarias para el desarrollo de la actividad de la empresa, para que los trabajadores no puedan acceder y empleen su tiempo más eficientemente en actividades propias de la empresa.

Deberá cifrarse la información que circule a través de la red: Evitará que personal no autorizado puedan acceder a la información confidencial que circula a través de la red y la puedan manipular en contra de la organización.

USO DEL SOFTWARE

La instalación de software en el equipo deberá ser instalado solo por el personal del área de sistemas autorizado: Los usuarios no podrán instalar programas que no sean de la organización para realizar su trabajo diario, ya que pueden poner en riesgo los equipos y la seguridad de la red de datos.

Todos los equipos deberán tener configurado la opción de cierre de sesión después de un lapso de inactividad: Se preverá que usuarios no autorizados puedan acceder, modificar o borrar información confidencial, mientras el usuario no está en su sitio de trabajo.

Se permitirá únicamente instalar software licenciado a los equipos: Se borrará el software inútil y se dará buen uso de los recursos informáticos utilizando

únicamente el software licenciado, así se mejorará la seguridad de la red y se evitará la propagación de virus informáticos.

Todo software nuevo antes de ser instalado en el equipo deberá ser probado y evaluado: De esta forma se evitará un software defectuoso que pueda modificar la información o bloquee los equipos de la entidad y la red de datos será más eficiente y segura.

CONCLUSIONES

Se utilizó para el levantamiento de los activos de información de la empresa taller industrial Alkan S.A.S de la ciudad Guadalajara de Buga, Valle la metodología Magerit, logrando el inventario, clasificación de los diferentes activos de forma cualitativa y cuantitativa, cualificando los riesgos y medidas necesarias para minimizar el impacto de cualquier amenaza que llegue a materializarse.

Se aplicó en las pruebas de penetración la metodología Etical Hacking con la herramienta Kali Linux utilizando: Nmap, Wireshark, Metasploit, SqlMap y Ettercap, logrando asi la materialización de las debilidades con que cuenta la información de la empresa Taller Industrial Alkan como: puertos abiertos, contraseñas débiles, información sin cifrar, equipos de fácil acceso con cuentas abiertas, con el apoderamiento total del equipo con metasploit.

Cada vulnerabilidad encontrada se valoró de acuerdo a la metodología Magerit dando como resultado una visión más específica sobre los impactos que estos pueden generar en la información de la empresa la cual es un valioso activo.

En el planteamiento de estrategias para la reducción de los riesgos encontrados la empresa debe invertir en recurso económico periódicamente para que todo el personal de la empresa reciba una adecuada capacitación y actualización en las

áreas de seguridad informática y de los riesgos a que está expuesta, además de sus sistemas operativos y la base de datos. Todo el personal de la empresa tanto interno como externo que manipule información confidencial y sensible, debe comprometerse a protegerla, para evitar fugas de información, la cual pueda ser utilizada indebidamente.

Es importante que la empresa implante un sistema de monitoreo que permita ver en tiempo real lo que está ocurriendo en la red y si es posible instalar y configurar un firewall que permita detener cualquier posible ataque a las vulnerabilidades que la empresa posee para llegar a prevenir un siniestro.

La empresa debe estar más involucrada en cumplir y divulgar el cumplimiento de las políticas de seguridad implementadas por la empresa, además debe definir la forma clara los procesos y roles a las personas responsables del departamento de seguridad informática.

Se pudo dar solución al problema planteado de realizar pruebas de penetración a la infraestructura tecnológica de la empresa para identificar las vulnerabilidades del sistema operativo y base de datos de la empresa Taller Industrial Alkan S.A.S.

Se identificó que en la empresa Taller Industrial Alkan S.A.S. durante todo el proceso del proyecto se detectó que tienen vulnerabilidades, que no tienen implementado un sistema de seguridad informática (sistema operativo y base de datos), ni en su infraestructura, en la empresa se puede hacer penetración e identificar puertos que alguien con mayor conocimiento del tema pueda aprovechar y acceder a información que es vital para la empresa.