ESCANEO DE VULNERABILIDADES AL SERVIDOR PRINCIPAL DE LA EMPRESA CASO DE ESTUDIO

JORGE LEONARDO RAMIREZ RESTREPO
WILLIAMS AVILA PARDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2018

ESCANEO DE VULNERABILIDADES AL SERVIDOR PRINCIPAL DE LA EMPRESA CASO DE ESTUDIO

JORGE LEONARDO RAMIREZ RESTREPO
WILLIAMS AVILA PARDO

Proyecto de Grado para optar por el título:
Especialista en Seguridad Informática

Director Proyecto
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2018

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Santiago de Cali, 02 de mayo de 2018

Dedico este proyecto de grado fundamentalmente a Dios, quien en su infinita bondad y amor, me brindo la fuerza y sabiduría necesaria para cumplir una meta más en mi vida y los objetivos de este proyecto.

A mi madre Tulia Elvira Pardo Rodríguez, por brindarme apoyo en cada instante de mi vida, por enseñarme los valores que necesita un hombre para salir adelante y ser una persona de bien, por darme una razón para lograr mis metas, pero más que nada, por brindarme su inmenso amor.

A el señor Agustín Emilio Contreras Morales, quien en algún momento de mi vida me dijo "Tu puedes lograr todo lo que te propongas", por confiar en mí y por enseñarme a confiar en mí, por tantos valiosos consejos a lo largo de mi vida y por ser como un padre para mí.

Y por último pero no menos importante, a mí esposa Diana Carolina Arciniegas Rojas, quien me ha acompañado en mis triunfos y derrotas, en aquellas noches largas de estudio arduo, quien me brinda su amor, gracias a ella que con su compañía me permite retarme cada día, en búsqueda de alcanzar mis metas y recompensar su amor.

Williams Ávila Pardo

Dedico este proyecto de grado principalmente a nuestro creador Dios, quien me permite vivir cada día con las mejores condiciones de salud y darme la sabiduría de tomar las mejores decisiones en cada momento.

A mis padres Humberto Ramírez y Elizabeth Restrepo por su apoyo constante y comprensión en cada etapa de mi vida, educándome e inculcándome los valores necesarios para ser una persona con ética personal y profesional, quienes con su ejemplo de perseverancia y respeto han edificado quien soy hoy en día.

A cada uno de los tutores de la Universidad Nacional Abierta y a Distancia en los cursos que tome a nivel de pregrado y posgrado, de cada uno de ellos tome las mejores orientaciones y conocimientos, que forjaron cada una de las bases necesarias para adquirir el conocimiento necesario, el cual hoy en día me lleva a dar desarrollo a este proyecto.

Finalmente, a mi novia Eliana Julieth Sánchez Torres, por brindarme el apoyo, motivación suficiente en los momentos difíciles e impulsarme a nunca dejar atrás mis metas.

Jorge Leonardo Ramírez Restrepo

AGRADECIMIENTOS

Williams Avila Pardo y Jorge Leonardo Ramírez Restrepo agradecen a:

La empresa caso de estudio por permitirnos desarrollar este proyecto en tan importante entidad, por brindarnos los recursos y disponibilidad para aplicar los conocimientos adquiridos en este programa académico.

La Universidad Nacional Abierta y a Distancia por brindar educación para todos, donde desde su plataforma tecnológica y equipo docente, puso a nuestra disposición todo lo requerido para realizar un correcto desarrollo del proyecto.

A tutores e Ingenieros Luis Fernando Zambrano y Salomón González quienes nos brindaron la orientación desde sus conocimientos en los cursos Proyecto de Seguridad Informática I y II respectivamente, sin sus observaciones y apoyo tutorial no hubiese sido posible desarrollar a cabalidad este proyecto.

Esp. Ing. Freddy Enrique Acosta quien fue nuestro asesor de proyecto, con su orientación metodológica y su gran disponibilidad logramos cumplir todos los objetivos propuestos.

De igual manera agradecemos a todas aquellas personas que de una u otra forma permitieron la realización de este proyecto.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA[1]**:** circunstancias que potencialmente puede provocar pérdidas o daños. Se pueden entender como una vulnerabilidad del sistema que está expuesto a un ataque.

ANALISIS: se le conoce a la investigación imparcial y minuciosa de un hecho o fundamento, descifrándolo para su estudio o evaluación.

ATAQUE**:** aprovechamiento de la vulnerabilidad de un sistema. Generalmente, se produce desde fuera del sistema y con una intención deliberada de causar algún daño. (Sommerville, & Alfonso Galipienso, 2005)

AUTENTICACIÓN: protección de la información contra falsificaciones.

CONFIDENCIALIDAD[2]: mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos atreves de redes de comunicaciones. (Gómez Vieites, 2014).

CONTROL DE ACCESO: el control de acceso se ejecuta acorde a los niveles de seguridad y es puesto en marcha por medio de la administración de la red. En su ejecución se da la aprobación de acceso a un sistema informático, aquí el sistema verifica si concede o niega la petición de acceso del usuario, luego de verificar si las credenciales recibidas son las correcta y de acuerdo con su rol, si tiene los permisos de acceder en el sistema. Lo anterior de acuerdo con las políticas de control de acceso de una organización y/o aplicación web.

DISPONIBILIDAD[3]**:** la disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficiente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios. (Gómez Vieites, 2014)

---

[1] CHICANO TEJADA, Ester. Auditoria de seguridad informática. 1 ed. España: IC Editorial. 2014.
[2] GIMÉNEZ ALBACETE, José F. Seguridad en equipos informáticos. 1 ed. España: IC Editorial. 2014, p 13.
[3] GIMÉNEZ ALBACETE, José F. Seguridad en equipos informáticos. 1 ed. España: IC Editorial. 2014, p 13.

FASE: es el paso que se está desarrollando durante algún punto en particular de una investigación.

HACKER: sujeto que posee muchos conocimientos de informática, con los cuales realiza acciones que le permite ingresar ilegalmente a sistemas informáticos no propios y manejarlos a su conveniencia o propósito.

INTEGRIDAD[4]**:** la función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática. (Gómez Vieites, 2014).

LEY: es una norma jurídica determinado por la debida jurisdicción, en que se ordena o impide algo en conformidad con la justicia. No cumplirla traerá su debida sanción, conforme con lo establecido por la misma ante su no acatamiento.

MSPI (Modelo de Seguridad y Privacidad de la Información): el modelo de seguridad y privacidad de la información enmarca un ciclo de operaciones que enmarca cinco fases (Diagnostico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua.), cuyo objetivo es hacer que las entidades públicas en Colombia gestionen apropiadamente la protección y reserva en sus activos de información. Siendo este un documento que da los lineamientos necesarios para ejecutar una serie de buenas prácticas en seguridad informática.

NORMATIVAS DE SEGURIDAD**:** existen cantidades diferentes normas de seguridad que las empresas actualmente implementan para la seguridad de la información. Todas estas normativas persiguen los mismos objetivos, ya que están diseñadas para incluir a todas las unidades o departamentos que estructura a la empresa para obtener una seguridad mínima de la información procesada y transferida por el personal que hace parte de ella. Las normativas de seguridad, tienen la finalidad de presentar los lineamientos necesarios para que las empresas puedan implantar un sistema de gestión de la seguridad de la información. (Ramírez Montañez, 2015)

PENTESTING**:** método utilizado para evaluar el nivel de seguridad de una organización, donde quien realiza dicha evaluación simula ser un atacante real que aplica diversa variedad de técnicas y cuyo objetivo es encontrar vulnerabilidades 8conocidad o no) a partir de falencias en las configuraciones de los equipos o bien en distintos procesos o contramedidas, sean estos de índole técnica o no. (Staff, 2011)

[4] GIMÉNEZ ALBACETE, José F. Seguridad en equipos informáticos. 1 ed. España: IC Editorial. 2014, p 13.

RIESGO: el riesgo es la probabilidad de que una amenaza suceda, dando como resultado un ataque informático en un equipo o red informática.

SEGURIDAD INFORMATICA: es la disciplina que se preocupa por velar por la integridad y privacidad de los datos guardados en un sistema. Este tipo de protección se realiza a nivel físico y lógico, está apoyada por estándares de calidad y normativas internacionales.

SERVIDOR[5]: el concepto de servidor se aplica de forma genérica a equipos informáticos que suministran servicios de base de datos. (Desongles Corrales, 2005).

SISTEMA INFORMATICO: es el sistema cuyo propósito es de guardar y procesar información, está conformado por software, hardware y usuarios, los cuales interactúan de manera interrelacionada.

SISTEMA OPERATIVO[6]: es un programa que actúa como intermediario entre el usuario y el hardware de un sistema de cómputo. El propósito es ofrecer un ambiente en el que el usuario pueda ejecutar programas de una forma cómoda y eficiente. (Candela Solá, 2011)

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: es el eje central de donde se da desarrollo a la ISO 27001. Su propósito radica en salvaguardar la confidencialidad, integridad y disponibilidad de la información, al igual que todos los sistemas informáticos que están relacionados con la administración de la información en una organización.

VIRTUALIZACIÓN[7]: hace referencia a la emulación virtual de un componente tecnológico, este procedimiento se realiza con el fin de evitar trabajar con el dispositivo físico y/o para realizar pruebas a los mismos.

VULNERABILIDAD[8]: debilidad de in sistema informático para que se puede aprovechar para provocar pérdidas o daños. (Sommerville, & Alfonso Galipienso, 2005)

WINDOWS SERVER 2012[9]: durante muchos años Windows Server ha sido un sistema operativo que permite a las organizaciones de cualquier tamaño crecer y

[5] HERNÁNDES PÉREZ, Flor A, et al. Glosario de términos informáticos [en línea]. El Cid Editor Editorial, 2006. ISBN E-BOOK: 978-141-35-6491-4. p 87. [Consultado: 02 de noviembre de 2017]. Disponible en internet: http://bibliotecavirtual.unad.edu.co:2460/lib/unadsp/reader.action?docID=3167493

[6] CANDELA, Santiago et al. Fundamentos de Sistemas Operativos. 1 ed. España: S.A Ediciones Parainfo. 2007, p 2.

[7] HANDZ, Valentín. Windows 7 y sus Novedades. 1 ed. Handsofthelp. 7 p.

[8] AGUILERA, Purificación. Seguridad informática. 1 ed. España: Editex. 2010, p 14.

administrar su infraestructura de tecnología ofreciendo soluciones fáciles de usar, robustas y seguras. Partiendo de este legado, Microsoft anuncia Windows Server 2012, aportando su experiencia en la construcción y operación nubes públicas a la plataforma de servidor de nubes privadas; entregando cientos de nuevas funciones y mejoras que abarcan la virtualización, redes, almacenamiento de información, experiencia de usuario, computación en la nube, automatización y mucho más. ("Windows Server 2012 – Nuevo Licenciamiento", 2017)

[9] FLORES ROSA, Marco A. Windows Server R2. 1 ed. Perú: S.A Editorial Macro. 2014, 13 p.

RESUMEN

El servidor principal de la empresa caso de estudio, como todo sistema informático, está expuesto a que se presente ente un ataque informático, proveniente de terceros (externos o internos) que tengan algún interés en sustraer información de la empresa con el propósito de hacer daño, incluso haciendo caer los sistemas por un tiempo prolongado.

El delincuente informático o hacker posee los instrumentos y competencias necesarias para acceder un sistema informático, logrando evadir los controles de seguridad tradicionales y logrando así su objetivo. Por tal motivo se plantea realizar un Escaneo de Vulnerabilidades al servidor principal de la empresa caso de estudio, el cual permita identificar y evaluar cada uno de los riesgos que posee en la actualidad y de esta manera disminuir o evitar la probabilidad de que un ataque informático se presente en el futuro.

En el proyecto se utilizó software libre que permitió realizar todas las acciones de detección y reporte de informes necesarios para la toma de decisiones objetivas, que permitan salvaguardar el sistema y mejorar las políticas de seguridad informática dentro de la organización. Se realizó la revisión teórica y se hicieron las diferentes pruebas experimentales sobre sistemas similares con el fin de fortalecer las competencias en los autores del proyecto, para luego aplicarlas al desarrollo del proyecto.

El proyecto en su desarrollo se dividió en dos fases: la primera correspondiente a la identificación de vulnerabilidades en el servidor y la segunda donde se realizó la evaluación de las vulnerabilidades del servidor y se indicó la propuesta de procedimientos que permita mitigar las vulnerabilidades encontradas. Con los resultados generados se realizan la lista de recomendaciones a la empresa caso de estudio.

Palabras clave: servidor principal, ataque informático, sistema informático, pentesting, riesgos, vulnerabilidades.

ABSTRACT

The main server of the company case study, like any computer system, is exposed to a computer attack, from third parties (external or internal) that have some interest in subtracting information about the processes that are carried out in the Comptroller's Office or for the purpose of harming the State, even by causing the system to fall for an extended period of time.

The computer hacker or hacker has the necessary tools and skills to access a computer system, avoiding traditional security controls and achieving their goal. For this reason it is proposed to perform a Vulnerability Scan to the main server of the Enterprise Case Study, which allows to identify and evaluate each of the risks that it has at present and in this way to decrease or avoid the probability that a computer attack be present in the future.

The project uses free software that allowed to perform all the actions of detection and report reporting necessary for making objective decisions, which allow to safeguard the system and improve computer security policies within the organization. The theoretical review was carried out and the different experimental tests were done on similar systems in order to strengthen the competencies in the project authors, and then apply them to the development of the project.

The project in its development was divided in two phases: the first one corresponding to the identification of vulnerabilities in the server and the second one where the evaluation of the vulnerabilities of the server was made and the proposal of procedures was indicated that allows to mitigate the vulnerabilities found. With the results generated the list of recommendations is made to the Company Case Study.

Keywords: main server, computer attack, computer system, pentesting, risks, vulnerabilities.

INTRODUCCIÓN

El análisis y gestión de riesgos introduce un enfoque riguroso y consecuente para a investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas que afectan al sistema informático; y la determinación de la vulnerabilidad del sistema a dichas amenazas. Su objetivo es proporcionar una medida de las posibles amenazas y vulnerabilidades del sistema de manera que los medios de seguridad puedan ser seleccionados y distribuidos eficazmente para reducir al mínimo las posibles pérdidas.[10]

Durante estos últimos años se han descubierto multitud de fallos y vulnerabilidades en todos los sistemas operativos del mercado: las distintas versiones de Windows de Microsoft, las familias de Linux, MacOS, etcétera. Así mismo, se han descubierto numerosos vulnerabilidades en gestores de bases de datos como Oracle o SQL Server y, de hecho, una de ellas facilito la rápida propagación del virus SQL Slammer en el año 2003.

Por otra parte, no debemos olvidar las innumerables vulnerabilidades en otras aplicaciones y servicios críticos en muchas redes informáticas como los servidores Web (como Apache para el entorno UNIX/Linux o Internet Información Server para el entorno Microsoft), servidores FTP, servidores de correo electrónico ("Mail Transfer Agents", MTA) como Sendmail, etcétera.[11]

A causa de la necesidad de garantizar la confiabilidad en los sistemas informáticos de la entidad, acorde a las políticas de buenas prácticas en los Sistemas de Gestión de Seguridad de la Información (SGSI) y dando cumplimiento a los requisitos establecidos en la norma ISO 27001 del 2013.

Un sistema informático, debe velar por tres principios fundamentales en la seguridad de la información: integridad, confidencialidad y disponibilidad. En concordancia con lo anterior en este proyecto se planteó como objetivo principal identificar y evaluar las vulnerabilidades que atente contra los principios fundamentales de la seguridad Informática en el servidor de la empresa caso de estudio y plantear las medidas y procedimientos necesarios para mitigarlas.

Para lograr el completo desarrollo del objetivo propuesto, los autores planearon, diseñaron e implementaron un ambiente de pruebas, el cual les permitió identificar

[10] DE PABLOS HEREDERO, Carmen. IZQUIERDO LOYOLA. Víctor, LOPEZ. José Joaquín, AGUIS. Hermoso, Dirección y Gestión de los Sistemas de Información en la Empresa. Ed. Escuela Superior de Gestión Comercial y Marketing. (2006)
[11] GOMEZ VIETES. Álvaro. Enciclopedia de la Seguridad Informática. Ed. Ra-ma (2011)

las vulnerabilidades del servidor y posteriormente la evaluación de estas; este proceso concedió los criterios requeridos para establecer procedimientos para mitigar las vulnerabilidades encontradas.

El escaneo de vulnerabilidades tuvo como alcance único el servidor principal de la gerencia Valle del Cauca de la empresa caso de estudio, la cual, dispuso una serie de condiciones en aras blindar la seguridad de la organización y protegerla en caso tal que la información resultante de este proyecto fuese usada con fines no éticos. Con los resultados obtenidos, los autores sugieren a las partes interesadas, sobre los riesgos presentes en el sistema informático, basados en hallazgos, indicando las medidas correctivas y de contingencia acordes, que permiten garantizar el buen funcionamiento y protección de los datos almacenados en el servidor objeto de este proyecto.

Implementar el escaneo de vulnerabilidades, trae una serie de beneficios, entre los tres más relevantes: al empresa podrá definir la factibilidad real de un acceso no autorizado y el alcance que este tenga sobre la entidad; con los hallazgos se tiene la información suficiente para llevar a cabo la implementación de los controles de seguridad y disminuir los riesgos encontrados; se concientizo a la alta gerencia sobre la importancia de fortalecer la seguridad de los sistemas informáticos de la entidad.

.

1. DEFINICIÓN DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Como en toda compañía, es importante que la empresa caso de estudio cuente con información referente a las vulnerabilidades informáticas de su servidor principal y los servicios tecnológicos que en este se ejecutan y así, poder comparar el estado actual de la empresa contra lo dispuesto en los estándares internacionales tales como SOX, HIPPA, ISO27000, BS 7799[12]; estos estándares marcan el norte y referencia para medir el cumplimiento de los parámetros internacionales en materia de seguridad informática

La empresa caso de estudio cuenta con gerencias quienes se encargan de ejercer sus funciones en las regiones, entre estas la gerencia Valle de Cauca de la empresa caso de estudio en la cual se enmarcara el objeto del desarrollo de este proyecto. La empresa caso de estudio dispone de un servidor HP Proliant ML350p generación 8, el cual es el corazón de la infraestructura de TI, cumpliendo la función de brindar los servicios y procesos de apoyo que no están concentrados en el nivel central.

La organización no posee conocimiento de las vulnerabilidades que existen en el servidor de la gerencia Valle del Cauca servidor, por lo tanto, no les es posible determinar el impacto que tendría un ataque que logre identificar y explotar una vulnerabilidad; se hizo necesario planear y realizar un escaneo de vulnerabilidades que permitió evaluar la seguridad del servidor, plantear medidas y procedimientos que permitan mitigar las vulnerabilidades e informarlas al área encargada de la seguridad informática, quien es el área competente para la implementación de las acciones correctivas.

1.2. FORMULACIÓN DEL PROBLEMA

¿El servidor de la empresa caso de estudio, presenta vulnerabilidades que atente contra los principios fundamentales de la seguridad informática; y de ser así, cuales son las medidas y procedimientos que permiten mitigarlas?

[12] Metodología para la Detección de Vulnerabilidades en Redes de Datos. (2012). Información tecnológica.

1.3. OBJETIVOS

1.3.1. Objetivo general

Identificar y evaluar las vulnerabilidades que atente contra los principios fundamentales de la seguridad Informática en el servidor de la empresa caso de estudio y plantear las medidas y procedimientos necesarios para mitigarlas.

1.3.2. Objetivos específicos

- Identificar las vulnerabilidades del servidor de la empresa caso de estudio.
- Evaluar las vulnerabilidades del servidor de la empresa caso de estudio.
- Establecer procedimientos para mitigar las vulnerabilidades encontradas.

1.4. JUSTIFICACION

La empresa caso de estudio es una entidad importante. Teniendo en cuenta el uso masivo de recursos informáticos y la importancia de la información, resulta muy importante garantizar la seguridad de los servicios de TI de la entidad.

Existen estándares internacionales tales como SOX, HIPPA, ISO27000, BS 7799[13] los cuales le permiten a las empresas evaluar, diseñar y ajustar sus políticas de seguridad informática, pero para esto, es importante e imprescindible que la empresa caso de estudio realiza el escaneo de seguridad planteado en el proyecto, con el fin de contar con los insumos necesarios para una comparación de cumplimiento entre las medidas de seguridad implementadas y lo dispuesto en dichos estándares de seguridad.

Implementar un escaneo de vulnerabilidades le permite a toda organización identificar y dar solución a todas aquellas vulnerabilidades presentes en sus sistemas informáticos, anticipándose a los delincuentes informáticos y así evitar que logren ingresar a los sistemas, editando o eliminada información considerada como confidencial.

[13] FRANCO David A., PEREA Jorge L. y PUELLO Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos. vol.23 no.3 La Serena 2012.

El escaneo de vulnerabilidades como técnica permite salvaguardar un sistema informático a partir de los hallazgos; está ligado históricamente a los principios de la seguridad informática; en la década de los 80 y 90, se entendía por Seguridad Informática a las acciones que se encaminaban a resguardar los equipos informáticos a nivel de sistema operativo, siendo este tipo de seguridad de carácter lógico, logrando evitar que los sistemas no funcionaran correctamente en especial por la acción de virus informáticos.

Años después con la aparición del internet a nivel empresarial y global, trajo consigo la oportunidad tecnológica de realizar diferentes tipos de conexiones entre usuarios, lo cual genero la aparición de nuevos tipos de vulnerabilidades que podrían ser exploradas por los hackers, poniendo en riesgo la información almacenada y que se compartía a través de las redes informáticas.

En su publicación web López habla de la necesidad de proteger los sistemas informáticos:

> *"Es necesario para le empresa conocer en todo momento cuánto vale su activo más crítico y valioso, la información del negocio, y cuáles son las brechas de seguridad que podrían propiciar el acceso a la misma. Es necesario conocer el estado de la seguridad en todo momento a través de análisis de riesgos dinámicos que permitan identificar las principales amenazas y cuantificar los riesgos asociados a la materialización de las mismas, teniendo en cuenta varios factores clave: el valor de la información, la probabilidad de que una amenaza pudiera presentarse, y el impacto que tendría sobre el negocio la materialización de la misma."*[14]

La seguridad informática es fundamental en todas las organizaciones para garantizar la confidencialidad, integridad y disponibilidad de la información creada, almacenada y procesada en los sistemas de información. Por lo tanto se hace necesario y urgente que la empresa caso de estudio implemente un escaneo de vulnerabilidades al servidor principal que permita diagnosticar el nivel de seguridad informática e identificar las posibles vulnerabilidades existentes y así poder contar con las recomendaciones de controles a implementar en cada uno de los hallazgos encontrados y tener las herramientas sólidas para definir medidas técnicas que permitan detectar posibles problemas que atenten a la información en medios informáticos y también definir controles y mecanismos para reducir los riesgos que atenten contra la misma.

[14] LOPEZ, David. Evolución de la Seguridad Informática [En línea]. Grupo Control Seguridad. Párr. 6. [Consultado: 06 de noviembre de 2017]. Disponible en Internet: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

1.5. ALCANCE Y DELIMITACION DEL PROYECTO

1.5.1. Alcance

El presente proyecto aplicado se encuentra entre los proyectos de gestión de la seguridad y lo que pretende es identificar y evaluar las vulnerabilidades que atente contra los principios fundamentales de la seguridad Informática en el servidor de la empresa caso de estudio, planteando medidas y procedimientos necesarios para mitigarlas

Se plantearan las medidas y procedimientos necesarios para mitigar las vulnerabilidades halladas producto del escaneo de vulnerabilidades realizado. La implementación estará limitada a la aprobación y autorización del área encargada de la seguridad informática, evento que no depende de los autores del proyecto.

El desarrollo de este proyecto se llevará a cabo en la ciudad de Santiago de Cali, en la empresa caso de estudio, durante el año 2017.

1.5.2. Limitaciones

Es conveniente resaltar que en el desarrollo del presente proyecto aplicado se pueden llegar a tener una serie de limitaciones que se describen a continuación:

- La empresa solicita que se firme acuerdo de confidencialidad entre los autores y el asesor, por ende, no se referenciara el nombre de la entidad.

- Por acuerdo de confidencialidad no se permitirá mostrar el direccionamiento IP público y privado de la entidad.

- No se tendrá en cuenta la solución para la mitigación de los riesgos producto de las vulnerabilidades halladas, debido a que la empresa caso de estudio no lo permite a causa del acuerdo de confidencialidad.

- Teniendo en cuenta la relevancia e impacto del proyecto para la empresa caso de estudio y la sensibilidad de la información que se tendrá como insumo para el desarrollo del mismo, los autores solicitaron la autorización y suscribieron un acuerdo de confidencialidad con el área encargada de la seguridad informática, con el fin de garantizar la seguridad informática. Esté documento no hace parte integral del proyecto con la finalidad de salvaguardar la identidad la empresa.

- El proyecto se ceñirá a todas las limitaciones consideradas por la empresa caso de estudio en pro de salvaguardas su integridad y seguridad informática.

- La empresa caso de estudio por acuerdo de confidencialidad avalara la publicación del documento en el repositorio institucional de la Universidad Nacional Abierta ya Distancia – UNAD.

1.6. METODOLOGIA DE INVESTIGACION

1.6.1. Unidad de análisis

En el desarrollo del presente proyecto aplicado se tomó como unidad de análisis a la filial Valle del Cauca que tiene la entidad caso de estudio a nivel nacional, lo que permitió medir la eficiencia, integridad, pertinencia y confiabilidad de la seguridad informática del servidor principal de la filial Valle del Cauca en la empresa caso de estudio.

1.6.2. Población y muestra

1.6.2.1. Población

El proyecto aplicado se centra en el servidor principal de la filial que se encuentra ubicada en la ciudad de Santiago de Cali.

1.6.2.2. Muestra

En el proyecto aplicado no se determina una muestra, debido a que se debe trabajar con el total de la población que para el caso de este proyecto es el servidor principal de la filial Valle del Cauca de la empresa caso de estudio.

1.6.3. Estudio metodológico

El desarrollo de este proyecto aplicado se realizó en dos fases, las cuales garantizaran el correcto cumplimiento de los objetivos planteados:

1.6.3.1. Fase 1: Identificación de las vulnerabilidades del servidor

Para el desarrollo de la fase 1 correspondiente a la identificación de vulnerabilidades del servidor se realizara una copia de seguridad del sistema operativo del mismo con el fin de evitar los efectos colaterales que puedan generarse producto del escaneo de vulnerabilidades. Hecho esto, se usan herramientas como: OPENVAS, NESSUS, NMAP y Microsoft Baseline Security Analyzer los cuales son software que permiten la identificación de vulnerabilidades en equipos de cómputo y servidores.

1.6.3.2. Fase 2: Evaluación las vulnerabilidades del servidor y propuesta de procedimientos para mitigar las vulnerabilidades encontradas

Previamente identificas las vulnerabilidades del servidor principal de empresa caso de estudio se procederá a realizar la evaluación de las mismas con el fin de diseñar y proponer los procedimientos que permitan la mitigación del riesgo que conlleva contar con estas vulnerabilidades.

1.6.4. Instrumentos de recolección de información

El instrumento utilizado para la recolección de información en el desarrollo del proyecto aplicado se utilizó el software para copias de seguridad del sistema operativo Windows Server 2012 que posee el servidor principal de la empresa caso de estudio.

1.6.5. Producto resultado a entregar

En el proyecto aplicado encontrará las medidas y procedimientos necesarios para mitigar las vulnerabilidades halladas producto del escaneo de vulnerabilidades realizado al servidor principal de la filial Valle del Cauca de la empresa caso de estudio, las cuales han sido entregadas al área encargada de la seguridad informática, para su aprobación e implementación.

1.6.6. Tipos de investigación

A continuación se hace una breve descripción de los tipos de investigación utilizados en la presente monografía:

1.6.6.1. Investigación Descriptiva

A través de un estudio descriptivo se pretende obtener información acerca del estado actual de los fenómenos. Naturalmente, recabar toda la información posible acerca de un fenómeno, se antoja como meta difícilmente alcanzable, pero, de acuerdo con los propósitos de estudio, el investigador determina cuales son los factores o variables cuya situación pretende identificar.[15]

1.6.6.2. Investigación Proyectiva

La esencia de la investigación proyectiva consiste en proyectar hacia el futuro un modelo de comportamiento obtenido de la observación de un conjunto de variables representativas en un fenómeno y ligadas entre si por una relación funcional significativa.[16]

1.6.6.3. Investigación Evaluativa

Shuman citado por Pérez indica que la investigación evaluativa se constituye en una modalidad de la investigación que no se orienta como la investigación ordinaria o básica a la teoría, a la generación de conocimiento, sino a la valoración y al logro de resultados eminentemente útiles.[17]

[15] MORENO BAYARDO María Guadalupe. Introducción a la Metodología de la investigación educativa, (2005)
[16] REVISTA DE EDUCACIÓN. XIX Volumen LXXVII números 215-216. Madrid, España. (1971)
[17] PEREZ JUSTE Ramón. Ed. LA MURALLA, (2013)

2. MARCO REFERENCIAL

2.1. MARCO TEORICO

2.1.1. Estado del arte de la seguridad informática en Colombia

La constante innovación de las últimas décadas, producto de los avances tecnológicos, trae consigo numerosas ventajas para los usuarios en diferentes contextos, pero a su vez ha traído consigo una problemática que afecta a miles de personas a diario, la falta de seguridad informática en los sistemas de información, sean físicos o lógicos.

En Colombia de acuerdo a los datos de la Fiscalía el delito informático incremento en un 60% durante el 2016, según la información suministrada por el diario Portafolio, el más importante en temas de economía y negocios" El cibercrimen representa el 15% de los ilícitos cometidos a empresas en Colombia. Pérdidas anuales son cercanas a los 600 millones de dólares" [18](C. Tiempo, "La ciberdelincuencia no segmenta: todos somos vulnerables", Portafolio.co, 2017), las principales modalidades de delitos informáticos son:

- Descubrimiento y revelación de secretos
- Delitos contra la intimidad y el acoso
- Amenazas
- Falsificación
- Sabotaje informático
- Suplantación de identidad
- Delitos contra la propiedad intelectual

Siendo la información el activo más importante para una organización o usuario común, es un elemento que debe contar con todas las garantías de seguridad necesarias, los administradores de una red de datos deben establecer los parámetros de configuración acordes a las políticas de seguridad de la organización y que estos cumplan con los estándares de seguridad informática locales e internacionales.

Todo sistema informático por más medidas de seguridad que se tomen no es 100% seguro. Es necesario realizar una retroalimentación periódica la cual permita conocer las nuevas tendencias en ataques informáticos y como asegurar la información frente a posibles eventualidades. Empresa que considere que con contratar un servicio de seguridad informática una sola vez, ya asegura su

[18] C. Tiempo, "La ciberdelincuencia no segmenta: todos somos vulnerables", Portafolio.co, 2017

protección a largo plazo, está incurriendo en un gran error y desperdiciando sus recursos económicos, dicha protección será efectiva solo por un periodo corto de tiempo.

Hoy en día toda organización en sus procesos y actividades, dependen de la información depositada en sus sistemas informáticos, al igual que el soporte oportuno y efectivo, de toda su tecnología, logrando asegurar el almacenamiento, procesamiento, distribución y análisis de la misma. Si una empresa es víctima de un ataque informático, está expuesta a tener pérdidas económicas inigualables, lo cual pone en duda la calidad y confidencialidad en el procesamiento de la información interna y externa, la cual es el compromiso de la empresa velar por la seguridad de la misma. Se hace entonces necesario contextualizar a los directivos de las organización, sobre el coste económico que conlleva asumir las consecuencias de un ataque informático, sabiendo de esta manera que la inversión en un sistema de información seguro es menor a comparación de los costos que sugiere atender un delito informático en sus sistemas de información, daños por desastres naturales, daños de terceros y demás que factores que atenten contra los tres principios fundamentales de la información: integridad, confidencialidad y disponibilidad.

Los resultados de la evaluación a un sistema informático deben evidenciar todos los elementos que presentan riesgos, definir el alcance de un ataque sobre los activos informáticos, de manera que la alta gerencia sea consiente, de las dificultades técnicas, operacionales y el impacto que se tiene sobre el negocio (pérdida de credibilidad hacia el cliente, ventaja competitiva de la competencia, polémicas).

Cuando se presenta un problema de seguridad informática, este no puede ser atendido de manera aislada, toda la seguridad del sistema debe ser tratada desde el punto más débil hasta el más fuerte. La capacitación que se da a los usuarios del sistema es un punto clave al momento de garantizar la protección del mismo. Es claro que se puede contar con un gran esquema de seguridad informática en una empresa, pero si no se cuenta con una disposición apropiada por parte de los directivos de la organización y una cultura de buenas prácticas por parte de los usuarios, no será posible alcanzar las metas de seguridad informática al implementar su esquema de protección.

El esquema de seguridad informática debe velar por brindar protección a tres elementos fundamentales: software, hardware e información. Desde este principio fundamental, se encaminan todas las acciones, que permitan fortalecer un sistema informático, evitar que este sea objetivo de los delincuentes informáticos. El Especialista en Seguridad Informática, debe por ética profesional y convicción, brindar todas las alternativas de protección y no desestimar esfuerzos en realizar hallazgos que sugieran un riesgo o vulnerabilidad en el sistema auditado.

Los hallazgos de la evaluación de riesgos y vulnerabilidades a un sistema informático, permiten abarcar varios aspectos del proceso de almacenamiento, transferencia y clasificación de la información, la entidad debe velar por establecer unas políticas de seguridad de la informático, dentro de un marco legal, lo cual designe responsabilidades a todos los actores involucrados, en la gestión de la información; el administrador del sistema informático, debe garantizar que las configuraciones, medidas de contingencia y tiempo de respuesta frente a un ataque informático, sea acorde, de manera que no afecte el normal funcionamiento de los procesos de la organización; el usuario estándar debe ser consciente de las consecuencia de un mal uso de los equipos que almacenan información, ser capacitado sobre lo que es confidencialidad de la información y que la misma interesa solo a la organización, desde un sentido de pertenencia y ética profesional.

2.1.2. Metodologías de análisis de riesgos

Para llegar a obtener resultados, mediante una metodología, la cual parte de un método, en el caso de la seguridad informática, se conocen diferentes metodologías de análisis de riesgos, aplicables al escaneo de vulnerabilidades, estas son:

OSSTMM[19]: En ingles Open Sourse Security Testing Methodology Manual, en español Manual de la Metodología Abierta del Testeo de Seguridad; corresponde a un manual de metodología abierta diseñado para realizar pruebas de seguridad. Se convierte en uno de los estándares más completos y usados al momento de evaluar la seguridad de un sistema informático, se encuentra en continuo desarrollo, está compuesto por seis secciones:

Sección A -Seguridad de la Información
Sección B – Seguridad de los Procesos
Sección C – Seguridad en las tecnologías de Internet
Sección D – Seguridad en las Comunicaciones
Sección E – Seguridad Inalámbrica
Sección F – Seguridad Física

ISSAF[20]: Information System Security Assessment Framework (ISSAF) Es una metodología que permite realizar escaneo de vulnerabilidades, ha sido desarrollada para identificar y evaluar una red de trabajo, sus sistemas y aplicaciones disponibles. Está compuesta por tres fases:

[19] ISECOM.ORG. (2017). ISECOM - Open Source Security Testing Methodology Manual (OSSTMM). [online] Disponible en: http://www.isecom.org/research/ [Accedido 29 Oct. 2017].
[20] OISSG.ORG. (2017). OISSG - ISSAF. [online] Disponible en: http://www.oissg.org/issaf.html [Accedido 29 Oct. 2017].

1. Planificación y Preparación
2. Evaluación
3. Reportes, Limpieza y Destrucción de Objetos

OWASP[21]: Open Web Application Security Project: Es un proyecto abierto, colaborativo, enfocado en la seguridad de las aplicaciones web. Compuesta por una comunidad mundial, dedicada a la mejora de la seguridad de las aplicaciones de software. Es comúnmente utilizada en procesos de auditoría de seguridad web, permitiendo hacer un análisis y evaluación de los riesgos.

2.1.3. Conveniencia del escaneo de vulnerabilidades en la empresa

Se convierte el escaneo de vulnerabilidades en una herramienta eficaz, la cual encuentra brechas de seguridad en las empresas. Siendo la protección de la información uno de las principales preocupaciones y retos de toda empresa, atender las amenazas que día a día se generan, no es tarea fácil, más aún cuando tales amenazas pueden provenir dentro de la misma organización; con intencionalidad o sin intencionalidad, están presentes. No se trata solo de encontrar un conjunto de amenazas, vulnerabilidades o riesgos, es tener la capacidad de predecir cuales nuevas se pueden generar o de qué manera el delincuente informático puede tomar alternativas de ingreso a un sistema informático, luego de ser descubierto. En términos de seguridad informática, así como en la guerra, se debe estar dos pasos más adelante que el enemigo.

Así como los ataques provienen desde dentro de la organización, también surgen desde el exterior, producto del ingenio de personas expertas en temas informáticos, quienes logran encontrar brechas de seguridad sin necesidad de estar conectado en un principio directamente dentro del sistema informático. Es aquí donde el escaneo de vulnerabilidades entra en juego, al momento de combatir las brechas de seguridad que posee un sistema informático y que una empresa no tiene presentes.

El interrogante que surge es ¿De qué manera puede una empresa tomar acciones preventivas frente a eventuales ataques informáticos? Existen diferentes mecanismos, como establecer controles en el acceso a la información, red de datos. Además, se generan escenarios simulados de posibles ataques informáticos, lo cual conlleva identificar y hacer la medición de los riesgos, desde el exterior del sistema informático de una empresa.

De esta manera el escaneo de vulnerabilidades en su función, actúa como metodología de protección, mediante la simulación de un delito informático dentro

[21] OWASP.ORG. (2017). OWASP. [online] Disponible en: https://www.owasp.org/index.php/Main_Page [Accedido 29 Oct. 2017].

de un sistema informático en la empresa. Se realiza sin notificación previa a los integrantes de la organización, buscando objetividad y eficacia en los resultados del mismo. Pensando como lo haría un delincuente informático, este no avisara de ninguna manera que va realizar el o los ataques, así mismo se realiza durante una franja horaria en que la mayor parte de los usuarios del sistema están descuidados (en altas horas de la noche o en la madrugada)

En efecto lo mencionado es la esencia del escaneo de vulnerabilidades, simular el ciberataque, hacer diferentes tipos de pruebas como lo haría el atacante, descubriendo las vulnerabilidades de la empresa, que fallas de seguridad tiene, las cuales pueden ser explotadas por el atacante y de esta manera acceder, modificar o robar la información, poniendo en riesgo los datos. Con los resultados del escaneo de vulnerabilidades, se permite establecer la manera en cómo poder mitigar y ejercer control sobre estos fallos de seguridad y que no sean de conocimiento de un posible atacante.

El escaneo de vulnerabilidades, se debe realizar periódicamente, atendiendo las novedades y técnicas que los ciberdelincuentes emplean, es ahí donde parte la premisa de que ningún sistema será 100% seguro a través del tiempo.

Siendo consiente la alta directiva de una organización sobre qué hacer una inversión en seguridad informática, mediante soluciones como el escaneo de vulnerabilidades, es el mecanismo que le permite conocer sus vulnerabilidades y mejorar la calidad en sus procesos, visto desde el interior y exterior, aspecto que incide en la imagen y credibilidad como organización.

2.2. MARCO CONCEPTUAL

Durante los últimos años el tema de la seguridad informática ha despertado especial interés en la opinión pública, gerentes de empresas y profesionales en la materia, debido a los últimos ataques informáticos perpetrados a nivel mundial como el Ransomware, el Malware, Spyware, la Ingeniería Social, entre otros, estos han tomado su auge en los últimos meses. La otra cara del tema sugiere un impacto positivo, lo cual ha sugerido a más personas capacitarse en temas de ciberseguridad, ampliando la oferta de profesionales en Seguridad Informática y los mismos hagan parte de las empresas más importantes a nivel mundial, desde ahí se emplean todo tipo de estrategias que buscan la protección de la información que se almacena, trasmite, procesa y transfiere en sus sistemas informáticos.[22]

[22] TIEMPO, C. (2017). Seguridad informática, el reto empresarial del momento. [en línea] El Tiempo. Disponible en: http://www.eltiempo.com/archivo/documento/MAM-1676396 [Accedido 26 Nov. 2017].

Una de las técnicas empleadas por los profesionales en esta materia es el escaneo de vulnerabilidades, como paso inicial al fortalecimiento de las políticas de seguridad, implementación de los Sistemas de Gestión de la Seguridad Informática, entre otros aspectos que salvaguarden la información y no pase a manos de terceros no autorizados.

2.2.1. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT

Si bien ISO 27005 e ISO 31000 son los estándares más conocidos para la gestión de riesgos, existen otros instrumentos que están alineados con estos estándares y que facilitan a una empresa enfocarse en la implementación de herramientas y metodologías que satisfagan los requerimientos básicos de la administración de riesgos en sus sistemas de información.

En este sentido fue desarrollado MAGERIT, una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.[23]

2.2.1.1. Amenazas

Es posible definir una amenaza como una circunstancias que potencialmente pueden provocar pérdidas y/o daños físicos o lógicos dentro de una sistema informático; también se pueden entender como una vulnerabilidad del sistema que está expuesta a un ataque por lo tanto puede representar algún tipo de riesgo para el mismo.

De acuerdo a la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT, las vulnerabilidades que se hallaran en este proyecto estarán relacionadas con las vulnerabilidades de los programas (E.20) y Errores de mantenimiento / actualización de programas (E.21). [24] Ilustración 1.

[23] AMAYA, C. and Amaya, C. (2013). MAGERIT: metodología práctica para gestionar riesgos. [online]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ [Accedido 1 Dic. 2017].

[24] AMAYA, C. and Amaya, C. (2013). MAGERIT: metodología práctica para gestionar riesgos. (2017). [online] Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html [Accedido 3 Dic. 2017].

Ilustración 1 Tipos de amenazas a identificar en el proyecto

5.3.13. [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

Fuente: Libro II - Catálogo de Elementos - MAGERIT – versión 3.0

2.2.1.2. Vulnerabilidades

MAGERIT define una vulnerabilidad como *"toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza."*[25]

[25] CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA DE ESPAÑA. MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1. España. 2012.

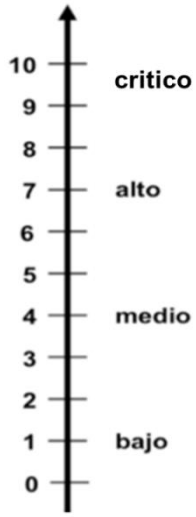
Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.[26]

2.2.1.3. Criterios de valoración del riesgo

Para realizar la valoración del riesgo de una vulnerabilidad MAGERIT propone que se use una escala común para todas las dimensiones, permitiendo comparar riesgos, esta escala deber ser logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas y se use un criterio homogéneo que permita comparar análisis realizados por separado

Atendiendo la sugerencia de MAGERIT, se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable y 10 como un valor relacionado a un daño extremadamente grave (a efectos de riesgo). Como se detalla en la ilustración 2 ambas escalas se correlacionan.[27]

Ilustración 2 Escala de valoración del riesgo



VALOR		CRITERIO
9 - 10	Critico	Daño extremadamente grave
6-8	Alto	Daño grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor

Fuente: Libro II - Catálogo de Elementos - MAGERIT – versión 3.0

[26] AMAYA, C. and Amaya, C. (2013). MAGERIT: metodología práctica para gestionar riesgos. [online] WeLiveSecurity. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ [Accedido 1 Dic. 2017].

[27] AMAYA, C. and Amaya, C. (2013). MAGERIT: metodología práctica para gestionar riesgos. [online] WeLiveSecurity. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ [Accedido 1 Dic. 2017].

2.2.2. ¿Qué es el escaneo de vulnerabilidades?

El escaneo de vulnerabilidades hace posible conocer las fallas que existen en un sistema operativo y su gama de servicios. Un escaneo de vulnerabilidades se puede hacer manualmente o empleando aplicaciones que hacen posible realizar el proceso y sus respectivos hallazgos.

Una prueba de análisis de vulnerabilidades es un análisis realizado a través de herramienta para verificar si el elemento analizado tiene vulnerabilidades reportadas en bases de datos como CVE. Cualquier persona puede ejecutar la herramienta y lo interesante corresponde al análisis de los resultados. Las herramientas más populares son Nessus y OpenVAS, estas son muy baratas y fáciles de usar. Con estas pruebas normalmente se identifican servicios sin clave, clave por defecto, servicios sin actualizar, ausencia de parches, entre otros.[28]

Siempre y cuando una empresa tenga definido cuáles son sus riesgos informáticos y la identificación de los mismos, será posible realizar la implementación de las acciones de carácter preventivo y correctivo, con el apoyo de un profesional o empresa, que realice la gestión y análisis de las vulnerabilidades de tipo informático que posea la empresa, brindado las soluciones que permitan prevenir y corregir los fallos de seguridad encontrados. Los soluciones preventivas y correctivas deben mantener el equilibrio entre el costo que tiene resolución de la vulnerabilidad, el valor del activo de información para la empresa y el nivel de criticidad de la vulnerabilidad.

2.2.3. Tipos de escaneo

Escáner de red y de puerto: aquí se aplica programas que han sido desarrollados para hacer el escaneo de una dirección IP, los puertos que se están abiertos, la red local, también aquellos servicios que no son confiables. Los resultados de emplear este tipo de software, permite identificar los puertos que están abiertos, los cuales serían una puerta de entrada a un atacante informático.

Escáner para la Seguridad de aplicaciones web: su propósito es hacer la evaluación de los riesgos presentes, de esta manera reconocer las vulnerabilidades que posea una aplicación web y de esta manera aplicar las medidas de contingencia que permitan evitar un futuro ataque.

Escáner de Base de datos: este tipo de escaneo hace posible identificar cuáles son los puntos débiles de un sistema de base de datos, permitiendo tomar

[28] GUITERREZ, Marcos. Diferencias entre Ethical Hacking, Análisis de vulnerabilidades, escaneo de puertos y otros [en línea]. Blog sobre informática y seguridad de la información. (26 de octubre de 2012). párr. 2. [Accedido: 03 de noviembre de 2017]. Disponible en internet: http://marcosjgutierrez.blogspot.com.co/2012/10/diferencias-entre-ethical-hacking.html

medidas, fortalecer las políticas de seguridad informática, de esta manera se vela por el activo informático más importante de toda organización.[29]

2.2.4. Herramientas más conocidas para el escaneo de vulnerabilidades

A partir del escaneo de vulnerabilidades, necesitaremos contar con otras aplicaciones denominadas escáneres de vulnerabilidades, que se encargan de identificar vulnerabilidades conocidas en los sistemas objetivos. Para hacerlo, cuentan con una base de datos de plugins encargados de llevar adelante este proceso de identificaciones. Cuando una vulnerabilidad nueva es reportada, se genera un nuevo plugin que permite identificarla y se agrega a la base de datos, una vez que esta es actualizada. Si la base de plugins está al día, la herramienta podrá detectar las últimas vulnerabilidades descubiertas hasta el momento de la actualización.[30]

A continuación, se indican las herramientas más comunes empleadas en un escaneo de vulnerabilidades:

NESSUS[31]: es una herramienta de análisis de vulnerabilidad de seguridad cuya funcionalidad es la de ayudar a detectar posibles vulnerabilidades en máquinas escaneadas. Nessus, un producto comercial de Tenable Network Security, es uno de los analizadores de vulnerabilidades más extendidos hoy en día. Utiliza una tecnología conocida como <<Nessus Professional-Feed>>, que, a su vez, es mantenido por un equipo experto en investigación y búsqueda de vulnerabilidades.

OPENVAS: está conformado por varios servicios y herramientas que ofrece una solución integral y potente en el análisis de vulnerabilidades y gestión de las mismas. Su entorno forma parte de la solución de gestión de vulnerabilidades comerciales de Greenbone Networks, desde la cual se han realizado desarrollos para la comunidad de código abierto desde 2009.

KALI LINUX: En el sistema operativo Kali Linux se emplean herramientas para el escaneo de vulnerabilidades tales como:

IKE-SCAN: es una herramienta de línea de comandos para el descubrimiento, identificación y prueba de sistemas IPsec VPN

NETDISCOVER: herramienta tipo activa/pasiva para el reconocimiento de direcciones ip locales y redes inalámbricas.

---

[29] METODOLOGÍA PARA LA DETECCIÓN DE VULNERABILIDADES EN REDES DE DATOS.. Información tecnológica. (2012)

[30] JARA, Héctor; PACHECO, Federico G. Ethical Hacking 2. Creative Andina Corp. 2009, p 108.

[31] DIAZ ORUETA, Gabriel et al. Procesos y herramientas para la seguridad de redes. 1 ed. España: Universidad Nacional de Educación a Distancia. 2014.

NMAP: es una herramienta de código abierto para exploración de red y auditoría de seguridad. Fue diseñado para escanear rápidamente redes grandes, aunque funciona bien contra hosts únicos. Nmap utiliza paquetes IP sin procesar de maneras novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos hosts, qué sistemas operativos (y versiones del sistema operativo) están ejecutando, qué tipo de filtros de paquetes / firewalls están en uso, y docenas de otras características. Aunque Nmap se usa comúnmente para auditorías de seguridad, muchos sistemas y administradores de red lo encuentran útil para tareas rutinarias como inventario de red, administración de programaciones de actualización de servicio y monitoreo de tiempo de actividad de host o servicio.

ZENMAP: Versión gráfica del scanner de puertos y servicios NMAP.

WIRESHARK: Es una herramienta para analizar protocolos y hacer análisis de trafico utilizado para revisar los paquetes en una comunicación.

2.3. ANTECEDENTES

Gonzales y Gómez en la Identificación de vulnerabilidades y diseño de políticas de seguridad para la aplicación web Sistema Integral de Registro Educación Permanente (SIREP) de la UNAD CCAV Cartagena, plantearon como objetivo identificar las vulnerabilidades en el aplicativo SIREP, efectuando pruebas y ataques con programas de escaneo, logrando como resultado encontrar las vulnerabilidades en la aplicación, conociendo de esta manera las debilidades del sistema, producto de esto mitigar los riesgos que se generan a partir de las vulnerabilidades. Este estudio es un antecedente importante para la presente investigación por cuanto aborda el mismo tema de estudio y puede ser tomado como un valioso referente desde lo conceptual y metodológico, ya que brinda especifica las herramientas a implementar para realizar el escaneo de vulnerabilidades, además que aplicación emplear para clasifica las vulnerabilidades encontradas y el estándar para analizar y evaluar los riesgos.[32]
Ayde Viver realiza un estudio sobre la identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de Pentesting. Aquí se determinaron las vulnerabilidades existentes en una red LAN, donde se pudo verificar el estado de la red, se aplicaron herramientas de pentesting y se hizo un análisis completo y detallado de la red LAN. Este estudio se puede tomar como referencia en cuanto a las

[32] : GONZÁLEZ POMBO, Alexandra Milena y GÓMEZ BARBOZA, Orlando. Identificar las vulnerabilidades en el manejo de la información y formular las políticas de Gobierno de Tecnología para el manejo seguro de la aplicación SIREP del CCAV Cartagena. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Cartagena. 2015.

instrucciones que contiene sobre las metodologías aplicadas en la búsqueda de vulnerabilidades en un sistema informático.[33]

Benavides y Velásquez, en su proyecto de grado Prueba de Intrusión al Sistema Operativo Windows Server 2003 de una Empresa del Sector Financiero, lograron desarrollar una prueba de intrusión al sistema operativo Windows Server, en donde mencionaron la clasificación de los diferentes tipos de ataques informáticos a los que está expuesto un servidor, las metodologías de prueba de intrusión, las herramientas a emplear para hacer el escaneo de vulnerabilidades, el plan de pruebas, la identificación de vulnerabilidades y los resultados de la investigación. Este documento sirve como referente en la medida que el mismo explica la fase escaneo de vulnerabilidades, siendo esta una de las etapas de un pentesting, teniendo presente que el alcance de nuestro proyecto solo llega hasta el escaneo posteriores resultados del escaneo realizado al servidor; de esta manera el documento hace las veces de guía.[34]

Guerrero, Lasso y Legarda en su proyecto de investigación 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. Realizaron pruebas de testeo a la red de datos para el diagnóstico de vulnerabilidades en el control de acceso al Sistema de Gestión Documental de la empresa INGELEC S.A.S, de acuerdo al dictamen revelado ejecutaron la evaluación y su impacto, de esta manera formalizaron un planteamiento de estrategias de mitigación de riesgos encontrados para la prevención y fortalecimiento de la seguridad en el control de acceso del Sistema de Gestión Documental. Este proyecto de investigación apoya el desarrollo de nuestro proyecto en la media de aquí se indican herramientas como OpenVAS (Sistema Abierto para Evaluación de Vulnerabilidades), la cual permite evidenciar la seguridad y las vulnerabilidades existentes en los sistemas de información, logrando de esta manera ser un apoyo metodológico en el desarrollo y análisis de los resultados del escaneo de vulnerabilidades en el servidor de la empresa caso de estudio.[35]

[33] VIVER RAMIREZ, Aydee Mercedes. identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de Pentesting. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Cali. 2016

[34] BENAVIDES ARIAS, Andrés Fernando y VELÁSQUEZ MAYORGA, John Freddy. Prueba de intrusión al sistema operativo Windows Server 2003 de una empresa del sector financiero. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Medellín. 2015.

[35] GUERRERO ERAZO, Henry Aldemar et al. 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. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Pasto. 2015.

2.4. MARCO LEGAL

2.4.1. Normatividad nacional

2.4.1.1. Ley 1273[36]

“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”

2.4.1.2. Ley 23[37]

“Sobre derechos de autor”

2.4.1.3. Ley estatutaria 1266[38]

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”

2.4.1.4. Ley 599[39]

“Por la cual se expide el Código Penal”

2.4.1.5. Ley 527[40]

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”

---

[36] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Diario Oficial 47.223. Bogotá. (Enero 5 de 2009)

[37] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 23 de 1982 Nivel Nacional. Bogotá. Diario Oficial. 28 de enero de 1982

[38] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266 de 2008 Nivel Nacional. Bogotá .Diario Oficial 47.2. 19 de diciembre 31 de 2008.

[39] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 DE 2000. Diario Oficial 44097. Bogotá. Julio 24 de 2000

[40] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527. Diario Oficial 43.673 del 21 de agosto de 1999. Bogotá. (Agosto 18 de 1999)

2.4.1.6. Constitución Política de Colombia[41]

Protección a la propiedad intelectual - Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

2.4.1.7. Decreto 1747[42]

"Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales."

2.4.1.8. Decreto 460[43]

Reglamentación del Registro Nacional de Derechos de Autor y regulación del depósito legal.

2.4.1.9. Decreto 1360[44]

"Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor."

2.4.1.10. Sentencia C-662[45]

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2.4.1.11. Documento CONPES 3854[46]

El cual reemplaza al Documento CONPES 3701 de 2011. En este nuevo documento se hace efectivo el deber de todas las entidades del Estado y sus actores involucrados a iniciar acciones que permitan prevenir y mitigar los riesgos informáticos. Además, se indica que se deben realizar jornadas de socialización

---

[41] COLOMBIA. . CONSTITUCION POLITICA DE COLOMBIA. Bogotá. D.C. 1991
[42] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1747 (11 de Septiembre). DIARIO OFICIAL No. 44.160, Bogotá, jueves 14 de septiembre de 2000. Bogotá. D.C. 2000
[43] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 460 (16 de marzo) Bogotá. D.C. 1995
[44] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1360 (23 de junio) Bogotá. D.C. 1995
[45] COLOMBIA, CORTE CONSTITUCIONAL, Sentencia C-662. Diario Oficial No. 48.308 Bogotá. (junio 6 de 2000)
[46] COLOMBIA, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL – CONPES. Documento CONPES 3854. Bogotá. (Julio 14 de 2011)

de contenidos que permitan al ciudadano conocer los riesgos informáticos, como prevenirlos y los pasos a seguir si se es víctima de alguno.

2.4.1.12. Acuerdo PSAA06-3334[47]

Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

2.4.1.13. Resolución 004256 - políticas de seguridad de la Universidad Nacional Abierta y a Distancia UNAD[48]

La Universidad Nacional Abierta y a Distancia (UNAD) es un ente universitario autónomo del orden nacional, con régimen especial, cuyo objeto principal es la educación abierta y a distancia, vinculado al Ministerio de Educación Nacional. La Universidad mediante Resolución 004256 del 3 de marzo de 2015, define las políticas en cuanto a Seguridad de la Información.

2.4.2. Normatividad internacional

A nivel internacional existen estatutos que garantizan la integridad, confidencialidad y disponibilidad de la información y sanciona a aquellas personas que osen incumplirla, entre los que se encuentran.

2.4.2.1. RFC 2196 (Site Security Handbook) [49]

Es una guía para el desarrollo de políticas y procedimientos de seguridad informática para los sitios que tienen sistemas en Internet.

2.4.2.2. ISO / IEC 27001 [50]

Es un estándar ISO para la formalización de un Sistema de Gestión de Seguridad de la Información (SGSI). Como la norma ISO / IEC 27001 no es un documento de libre acceso y puede ser que sea difícil para las organizaciones a entender y aplicar la norma ISO / IEC" (RFC 2196, 2014). Este manual es base fundamental para el desarrollo de políticas de seguridad en todo el mundo. El estándar ISO

[47] RAMA JUDICIAL DEL PODER PÚBLICO CONSEJO SUPERIOR DE LA JUDICATURA. Sala Administrativa. Bogotá. (marzo de 2006)
[48] UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD. Resolución 004256. (3, marzo, 2015). Por la cual se define las políticas del Marco de Referencias del SGSI. Bogotá. 2015
[49] EE. UU, INTERNET ENGINEERING TASK FORCE (IETF), RFC 2196 – Site Security Handbook. Fremont, California. (Diciembre 3 de 2014)
[50]ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27001. Ginebra, Suiza. (octubre de 2013)

2700x establece “Control y la certificación de seguridad de la información en la empresa. Las empresas tienen que buscar esta certificación para obtener la calidad y cumplimiento en sus departamentos de Tecnología de la Información / Sistemas de Información.” (ISO 2700x *Security Standards*, 2011). Es altamente usado ya que se adapta a cualquier tipo de organización sin importar su actividad o tamaño.

2.4.2.3. ISO/IEC 17799 [51]

El cual “establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Los objetivos trazados proporcionan una guía general sobre los objetivos comúnmente aceptados de gestión de la seguridad de la información. Contiene las mejores prácticas de los objetivos de control y controles en las siguientes áreas de gestión de seguridad de la información:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Recursos humanos de seguridad.
- Seguridad física y ambiental.
- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Sistemas de información de adquisición, desarrollo y mantenimiento.
- Información de gestión de incidentes de seguridad.
- Gestión de la continuidad del negocio.

2.4.2.4. La convención sobre la propiedad intelectual de Estocolmo[52]

El Convenio de la OMPI, el instrumento constitutivo de la Organización Mundial de la Propiedad Intelectual (OMPI), fue firmado en Estocolmo el 14 de julio de 1967, entró en vigor en 1970 y fue enmendado en 1979. La OMPI es una organización intergubernamental que en 1974 pasó a ser uno de los organismos especializados del sistema de las Naciones Unidas. La OMPI tiene dos objetivos principales. El primero de ellos es fomentar la protección de la propiedad intelectual en todo el mundo. El segundo es asegurar la cooperación administrativa entre las Uniones que entienden en materia de propiedad intelectual y que han sido establecidas en virtud de los tratados administrados por la OMPI.

---

[51] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 17799. Ginebra, Suiza. (junio de 2005)

[52] ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL (2017). [online] Disponible en: http://www.wipo.int/treaties/es/convention/summary_wipo_convention.html [Accedido el 7 Nov. 2017].

3. IDENTIFICACIÓN DE LAS VULNERABILIDADES DEL SERVIDOR

Para realizar el diseño de un ambiente de pruebas controlado y parametrizado que permita realizar el escaneo de vulnerabilidad, se debe garantizar la virtualización del sistema operativo objeto del análisis, evitando comprometer la integridad del servidor que se encuentra prestando los servicios de TI, con este diseño se identificaron posibles vulnerabilidades del servidor principal de la empresa objeto de estudio.

3.1. DISEÑO DEL AMBIENTE DE PRUEBAS.

Se creó un ambiente de pruebas que permite evitar posibles daños al servidor operativo y así poner en riesgo la disponibilidad e integridad de los servicios de TI.

En la ilustración 1 se puede apreciar el diseño del ambiente de pruebas, el cual está conformado por dos equipos de cómputo, el equipo que escaneara las vulnerabilidades y otro que permitirán virtualizar a través de la herramienta VirtualBox el sistema operativo del servidor. En la siguiente grafica se ilustra la estructura del ambiente de pruebas.

Ilustración 3: Estructura del ambiente de pruebas

Fuente: Propiedad de los autores

3.1.1. Requisitos de hardware

En la tabla 1 se relacionan las especificaciones físicas básicas de los equipos que conforman el ambiente de pruebas en el cual se desarrolló el escaneo de vulnerabilidades.

Tabla 1 Características hardware ambiente de pruebas

EQUIPOS AMBIENTE DE PRUEBAS		
ESPECIFICACIÓN	**EQUIPO EVALUADOR**	**EQUIPO EVALUADO**
Marca	HP	HP
Modelo	ProBook 4430s	6200 Pro SFF
Tipo	Laptop	Desktop
Procesador	Intel Core i5	Intel Core i3
N° de Núcleos	4	4
Memoria RAM	4 Gb	4 Gb
Ancho de banda	110 Kbps	110 Kbps

Fuente: Propiedad de los autores

3.1.2. Requisitos de software

Para el correcto diseño y ejecución de los múltiples escaneos de vulnerabilidades enmarcados en el desarrollo del proyecto, se dispuso la instalación y configuración de diferentes herramientas de distribución y código libre, con el fin de garantizar el mayor cubrimiento e identificación de las posibles vulnerabilidades existentes en el servidor, tabla 2 y 3.

Tabla 2 Sistemas operativos del ambiente de pruebas

SISTEMAS OPERATIVOS DEL AMBIENTE DE PRUEBAS		
HERRAMIENTA	**VERSIÓN**	**DESCRIPCIÓN**
Windows 7	Professional – Service Pack 1	Este SO es el sistema empleado como anfitrión de los dos equipos que componen el ambiente de pruebas.
Windows Server	2012 R2- 64 Bits	El SO Windows Server 2012 R2 se instaló en una máquina virtual de VirtualBox y posterior se realizó el proceso de restauración de la copia de seguridad objeto de la evaluación.
Kali Linux	Versión 2017.2-amd64	Es sistema operativo se usó para instalar y ejecutar las herramientas, OpenVAS, NMAP y Microsoft Baseline Security Analyzer.

Fuente: Propiedad de los autores

Tabla 3 Caracterización software del ambiente de pruebas

SOFTWARE AMBIENTE DE PRUEBAS				
HERRAMIENTA	**A**	**B**	**VENTAJAS**	**DESVENTAJAS**
VirtualBox versión 5.1.30	X	X	✓ Es una herramienta gratuita. ✓ Ahorro de costos, haciendo posible que no sea necesario invertir en más estaciones de trabajo, cuando se puede emular una o más estaciones de trabajo, desde un mismo equipo. ✓ Hace las veces de entorno de pruebas, sin afectar los archivos y configuración del sistema operativo anfitrión. ✓ Amplia compatibilidad con el hardware. ✓ Es multiplataforma.	× Requiere de un equipo informático potente y con gran rendimiento, de manera que pueda soportar los procesos de dos o más sistemas operativos al tiempo. × El sistema anfitrión debe ceder recursos como espacio en disco duro, memoria RAM o número de procesadores a los sistemas operativos emulados en la máquina virtual.
Nessus Vulnerability Scanner versión 6.11.1 de 64 bits	X		✓ Herramienta fácil de usar y práctica. ✓ Define el nivel de las vulnerabilidades (critica, alta, media, baja e informativa}. ✓ Gran cantidad de plugins para el análisis. ✓ Rapidez en términos de tiempo en sus escaneos. ✓ Puede hacer escaneos sobre aplicaciones web.	× Para acceder a todas sus funciones se debe contar con una versión paga.
OpenVAS	X		✓ Herramienta gratuita. ✓ No tiene un límite de direcciones IP en sus escaneos. ✓ Puede hacer escaneos sobre aplicaciones web.	× Complejidad de instalación y configuración. × Poca cantidad de plugins. × No detecta vulnerabilidades críticas.

A: Equipo Evaluador B: Equipo Evaluado

Fuente: Propiedad de los autores

Tabla 3 (Continuación)

HERRAMIENTA	A	B	VENTAJAS	DESVENTAJAS
NMAP	X		Es una herramienta de código abierto. ✓ Multiplataforma. ✓ Realiza escaneos que arroja resultados que no pueden ser detectados a simple vista por un usuario o administrador de red. ✓ Detecta puertos abiertos, cerrados, información sobre sistema operativo. ✓ Identifica que computadoras están conectadas a una red. ✓ Lista los servicios que se ejecutan en una máquina.	× Escanea solo una IP al tiempo. × De acuerdo a la complejidad del tipo de escaneo, este tardara. × La velocidad del escaneo está sujeta a la capacidad de rendimiento del equipo donde se está ejecutando.
Microsoft Baseline Security Analyzer 2.3	X		✓ Herramienta gratuita. ✓ Permite mejorar los procesos de administración en la seguridad informática. ✓ Detecta errores de configuración de seguridad y de actualización de seguridad. ✓ Compatible con todas las plataformas de Windows. ✓ Realiza el análisis de las contraseñas de las cuentas de usuario e indica si estas son vulnerables. ✓ Analiza el servidor IIS. ✓ Analiza las bases de datos.	× Solo puede ser ejecutada en sistemas operativos Windows. × Su funcionalidad está enfocada hacia las pymes. × Requiere que quien administre la herramienta tenga conocimiento avanzado en redes y administración de sistemas operativos Windows. × No está disponible en español.

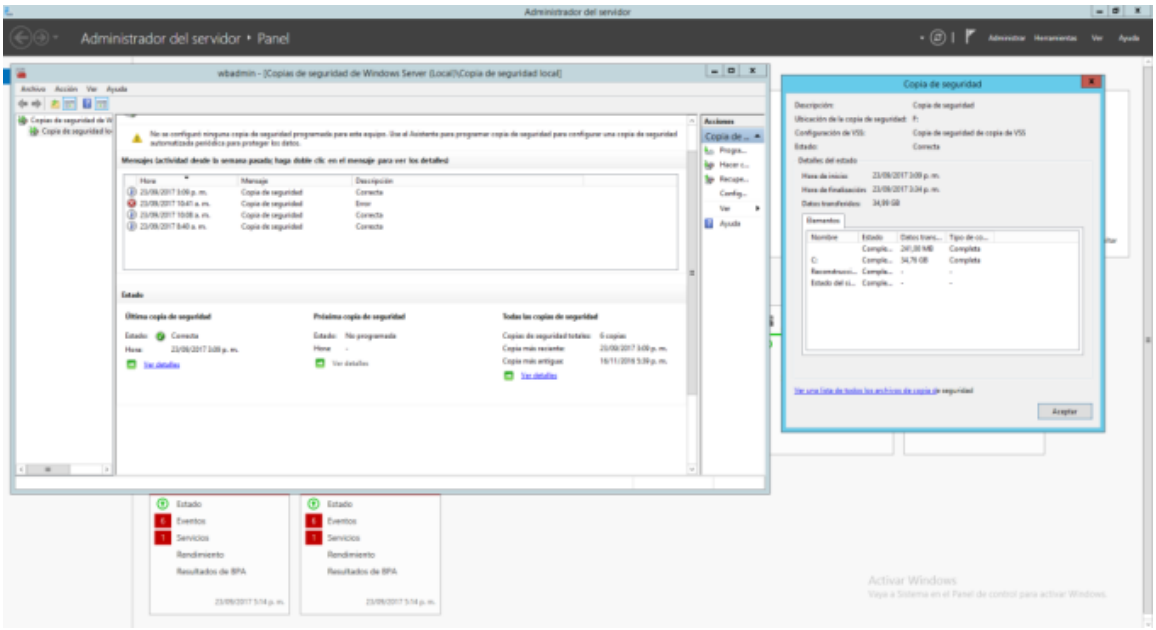
A: Equipo Evaluador B: Equipo Evaluado

Fuente: Propiedad de los autores

3.2. GENERACIÓN DE COPIA DE SEGURIDAD DEL SERVIDOR PRINCIPAL

Para la generación de la copia de seguridad del servidor se usó el servicio “Copias de Seguridad de Windows Server”; en la ilustración 2 se puede apreciar que la copia de seguridad se realizó omitiendo la unidad en la cual se encuentra almacenada la información del servicio de repositorio de archivos, ya que esta información no es relevante para la ejecución del escaneo de vulnerabilidades.

Ilustración 4: Generación de Copia de Seguridad



Fuente: Propiedad de los autores

3.3. CREACIÓN DEL AMBIENTE DE PRUEBAS

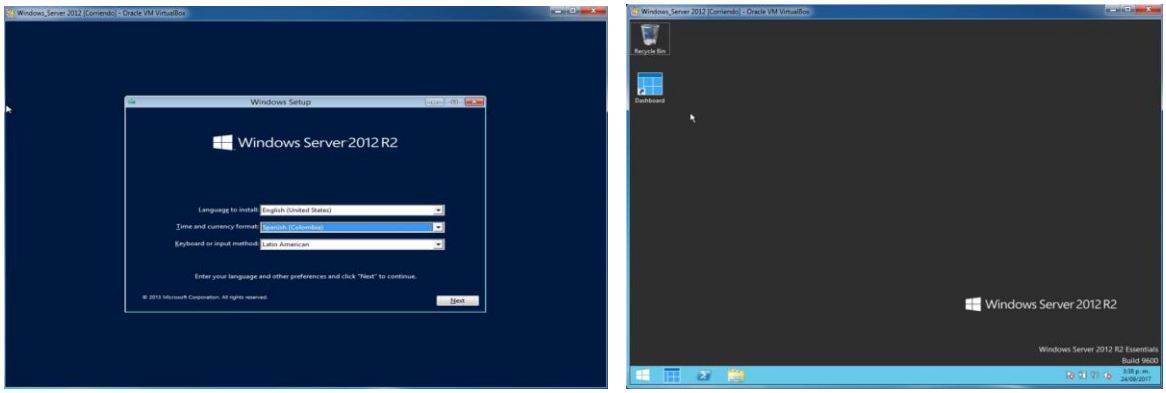
3.3.1. Instalación y configuración del ambiente de pruebas en el equipo evaluado.

3.3.1.1. Instalación y restauración de Windows server 2012 R2

Para el ambiente de pruebas del equipo que será evaluado en búsqueda de vulnerabilidades de seguridad, se instaló el software de virtualización VM VirtualBox Versión 5.1.28 y se creó una máquina virtual para la instalación del

sistema operativo Windows server 2012 en su versión de 64 bits, teniendo en cuenta configurar el adaptador de red con la opción “Adaptador puente” para permitir la comunicación y con la maquina evaluada, esto es posible apreciarlo en la ilustración 3.

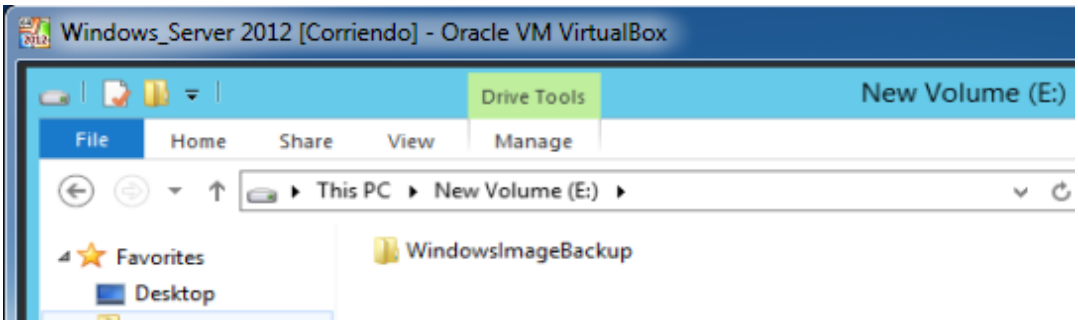
Ilustración 5: Proceso de instalación y virtualización de Windows Server 2012 R2



Fuente: Propiedad de los autores

Una vez fue instalado correctamente Windows Server 2012 R2 en la máquina virtual se creó una partición virtual del disco duro en la cual se alojó la copia de seguridad del servidor principal la cual permitió contar con una copia idéntica del servidor, lo cual garantizara que las vulnerabilidades halladas en este correspondan a la realidad.

Ilustración 6: Inserción de la copia de seguridad

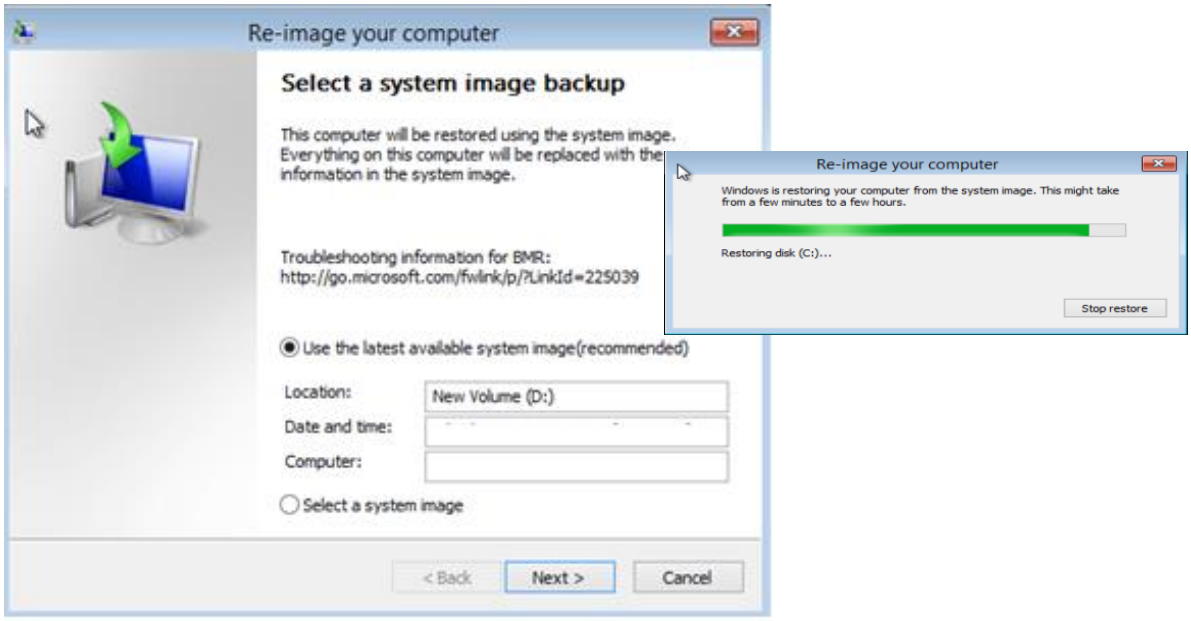


Fuente: Propiedad de los autores

La ilustración 5 muestra que una vez alojada la copia de seguridad en la máquina virtual se procedió a restaurarla, esto permitió contar con una copia idéntica del

servidor hasta el día 3 de noviembre del 2017 a las 12:09:18 PM, lo cual, es el estado idea para posteriormente realizar el escaneo de vulnerabilidades.

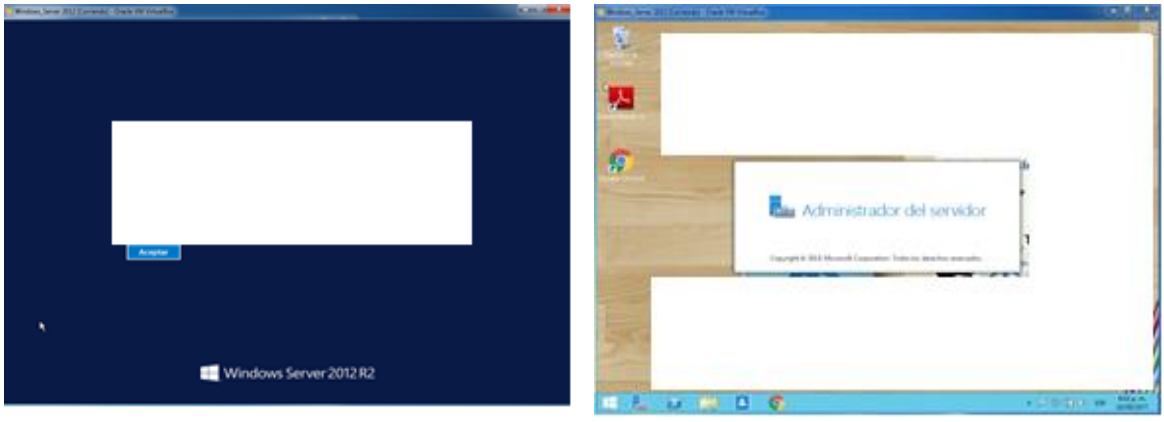
Ilustración 7: Restauración Copia de seguridad



Fuente: Propiedad de los autores

Terminado el proceso de restauración de la copia de seguridad en el ambiente de pruebas el servidor virtual quedo completamente operativo, ilustración 6.

Ilustración 8: Ejecución Windows Server 2012 R2 restaurado



Fuente: Propiedad de los autores

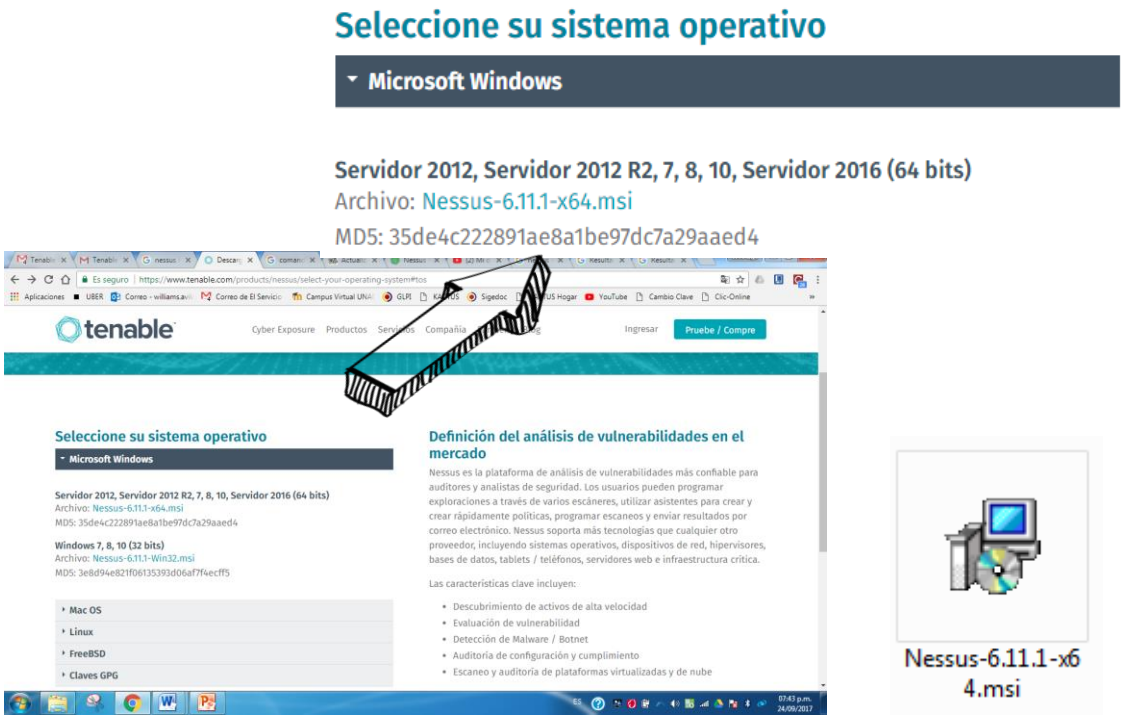
3.3.2. Configuración del ambiente de pruebas en el equipo evaluador:

3.3.2.1. Instalación y configuración Nessus Vulnerability Scanner

Para identificar las vulnerabilidades que posee el servidor, se ejecutara uno de los escaneos de vulnerabilidades usando la aplicación Nessus Vulnerability Scanner, esta es una aplicación web que permite la identificación de vulnerabilidades en una amplia gama de sistemas operativos. Nessus logra identificar las vulnerabilidades y riesgos que estas conllevan usando un daemon, el cual ejecuta el escaneo en el sistema y/o equipo objetivo, luego Nessus cliente (Este hace referencia a la aplicación de interfaz gráfica) muestra el avance e informa sobre el estado del escaneo.

Para ello descargamos la aplicación Nessus Versión 6.11.1 de 64 bits la cual es compatible con sistema operativos Microsoft Windows (Servidor 2012, Servidor 2012 R2, 7, 8, 10, Servidor 2016).

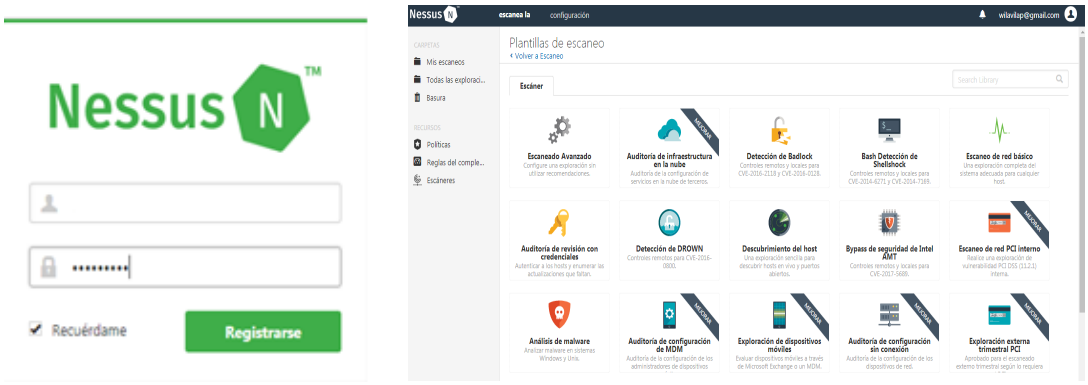
Ilustración 9: Configuración del ambiente de pruebas en el equipo evaluador:



Fuente: Propiedad de los autores

Finalizada la descarga y cómo es posible apreciar en la ilustración 8 se procedió a realizar la instalación y configuración de la misma, hecho esto y previo registro en la página de Nessus Home se procedió a ejecutar la aplicación para luego proceder al escaneo de las vulnerabilidades.

Ilustración 10 Instalación y configuración de Nessus

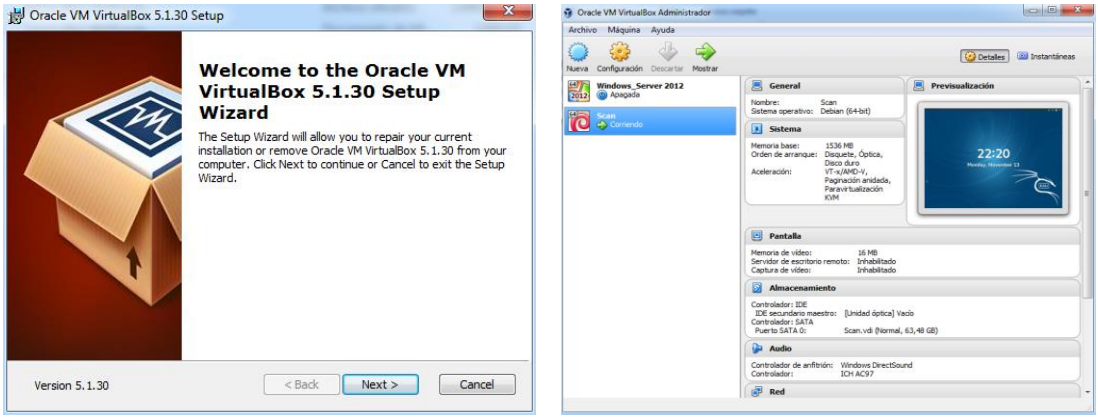


Fuente: Propiedad de los autores

3.3.2.2. Instalación del software de virtualización - VirtualBox

En la ilustración 9 se evidencia que para la creación de ambiente de pruebas se utilizó el software VirtualBox versión 5.1.30 el cual permite la creación de máquinas virtuales bajo el entorno del sistema operativo Windows, con el fin de realizar prácticas sobre otros sistemas sin afectar el sistema anfitrión, hecho esto se configuran las máquinas virtuales necesario para el desarrollo del proyecto.

Ilustración 11 Instalación VirtualBox

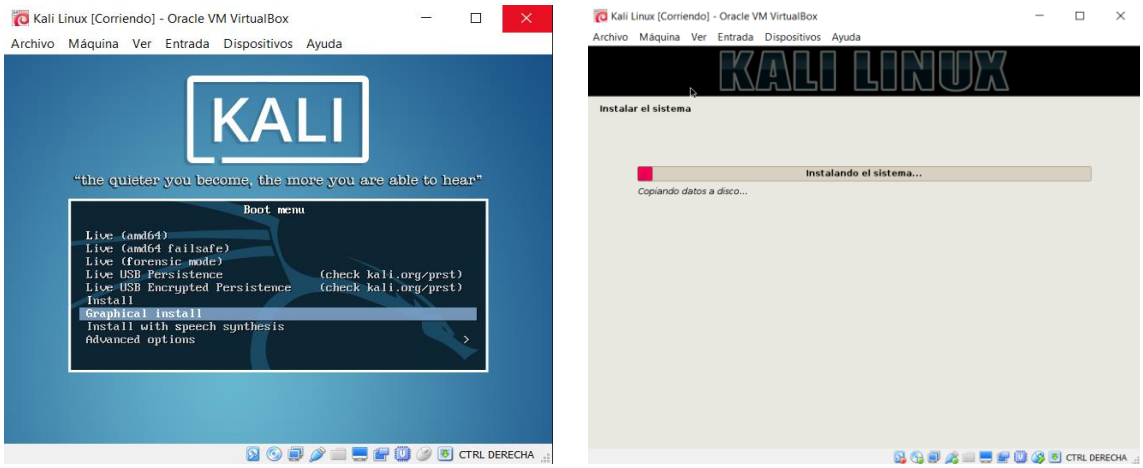


Fuente: Propiedad de los autores

3.3.2.3. Instalación Kali Linux

Para la instalación de Kali Linux, se escogió la opción del uso de un software de virtualización en este caso Oracle VM VirtualBox y se creó una máquina virtual para kali-linux-2017.2-amd64,esto es posible apreciarlo en la ilustración 10; se configuro el adaptador de red con la opción Bridged para permitir la comunicación y pruebas entre la máquina anfitrión (Windows 7) y la máquina virtual (kali-linux-2017.2-amd64).

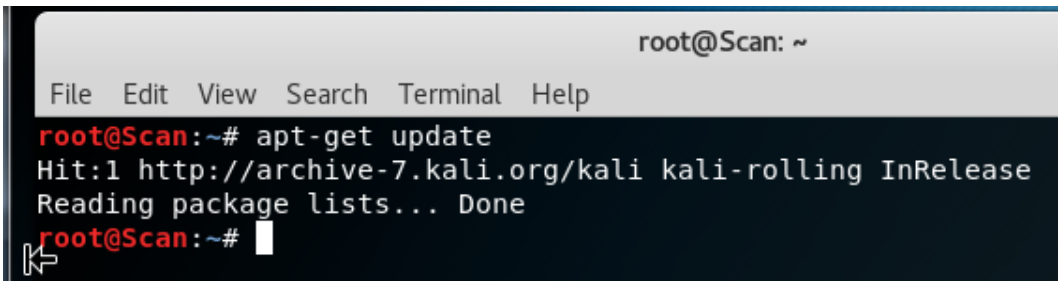
Ilustración 12 Instalación Kali Linux 2017-2



Fuente: Propiedad de los autores

Una vez instalado y configurado el sistema operativo Kali Linux se procedió a actualizarlo con la instrucción apt-get update, el cual permite obtener todos los cambios actuales del sistema para asi contar con la versión más reciente.

Ilustración 13 Actualización SO Kali Linux

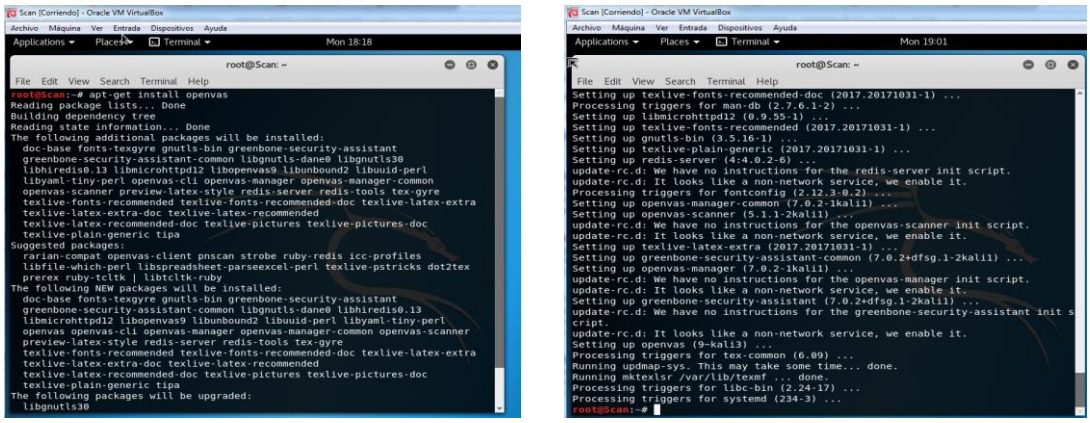


Fuente: Propiedad de los autores

3.3.2.4. Instalación y configuración de OpenVAS

Para confirmar las vulnerabilidades encontradas con el primer escaneo hecho con la herramienta, se ejecutara un segundo escaneo de vulnerabilidades usando la aplicación OpenVAS Vulnerability Scanner; a causa que OpenVAS ya no se encuentra preinstalada en Kali Linux, fue necesario instalarla, lo cual se puede realizar usando el comando apt-get install openvas, es posible apreciar todo este proceso en las ilustraciones 12, 13 y 14.

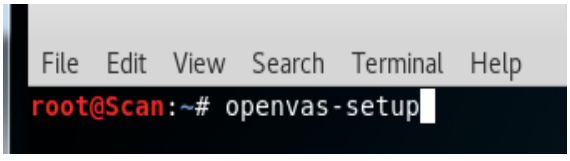
Ilustración 14 Instalación OpenVAS



Fuente: Propiedad de los autores

Una vez instalado OpenVAS se debió preceder a configurarlo, lo cual se realiza usando el comando openvas-setup, este comando hace que se ejecute la configuración atomatica.

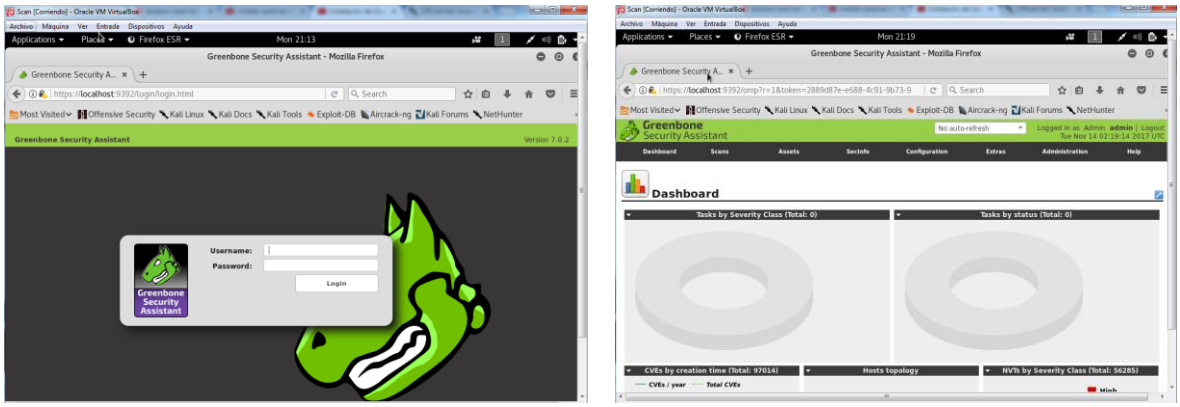
Ilustración 15 Configuración OpenVAS



Fuente: Propiedad de los autores

Finalizada la instalación y configuración de la herramienta y previo registro en la página de OpenVAS se procedió a ejecutar la aplicación para luego proceder al escaneo de las vulnerabilidades.

Ilustración 16 Instalación y configuración de OpenVAS

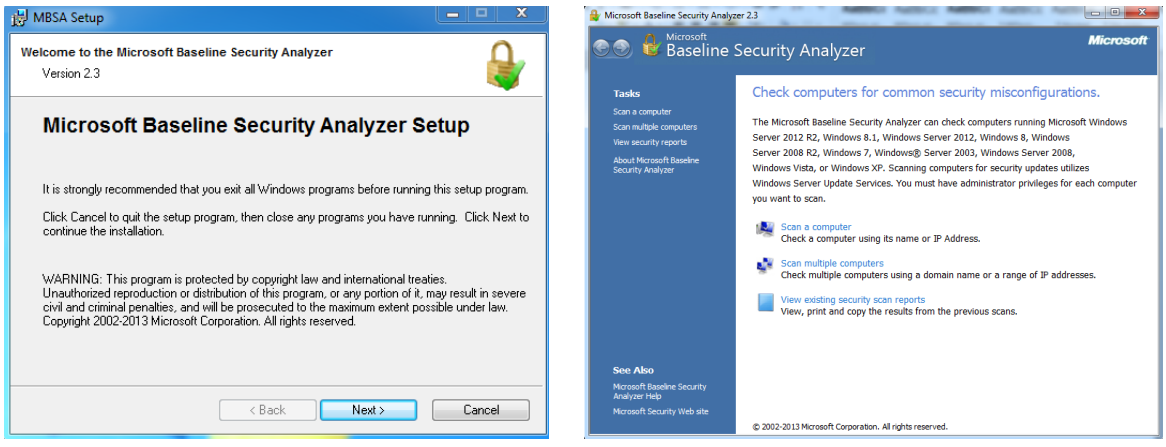


Fuente: Propiedad de los autores

3.3.2.5. Instalación y configuración de Microsoft Baseline Security Analyzer (para profesionales de TI)

Con el fin de identificar en el servidor posibles configuraciones de seguridad incorrectas, pack de servicios faltantes y parches de seguridad se instaló y configuro la herramienta Microsoft Baseline Security Analyzer 2.3 (para profesionales de TI), esta herramienta de distribución gratuita es ofrecida por Microsoft para evaluar fácilmente el estado de seguridad de las máquinas con sistemas operativos basados en Windows, MBSA incluye una interfaz gráfica y de línea de comandos que puede realizar escaneos locales o remotos de sistemas Microsoft Windows.

Ilustración 17 Instalación y configuración de Microsoft Baseline Security Analyzer



Fuente: Propiedad de los autores

3.4. ESCANEO E IDENTIFICACIÓN DE VULNERABILIDADES

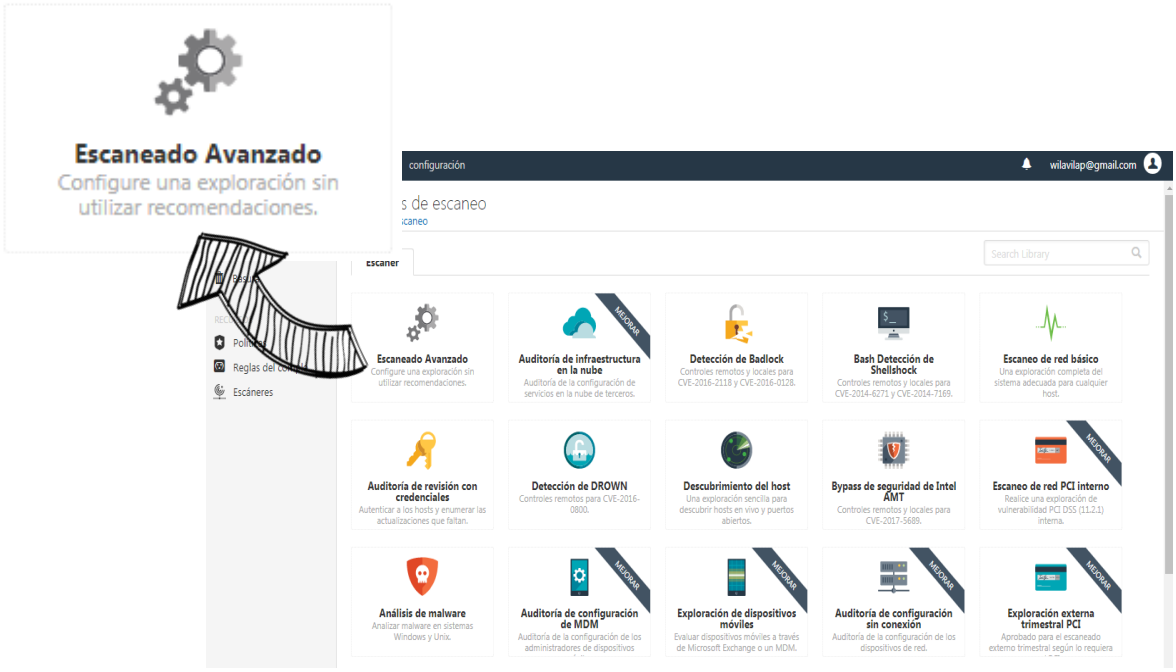
3.4.1. Configuración y ejecución de los escaneos de vulnerabilidades

3.4.1.1. Escaneo de vulnerabilidades con Nessus Vulnerability Scanner

Para la identificación de las vulnerabilidades del servidor con la herramienta Nessus Vulnerability Scanner se siguieron los siguientes pasos:

1. Se seleccionó la opción de Nessus “Escaneo Avanzado”. ilustración 16.

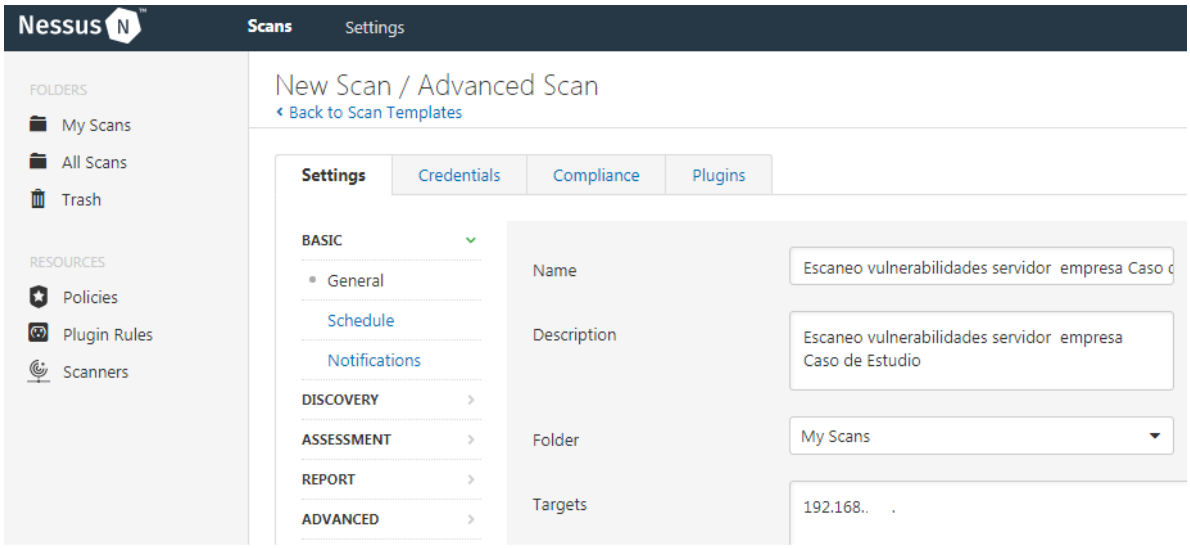
Ilustración 18: Configuración del escaneo de vulnerabilidades



Fuente: Propiedad de los autores

2. Para realizar el escaneo de vulnerabilidades debimos ingresar los siguientes parámetros: el nombre del escaneo el cual denominamos “Escaneo vulnerabilidades servidor empresa caso de estudio”, un breve descripción del mismo, la carpeta donde deseamos guardar la información y la dirección IP de la maquina a escanear. ilustración 17.

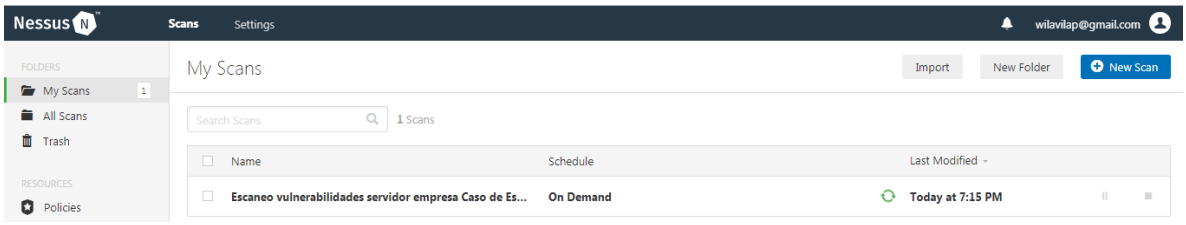
Ilustración 19: Descripción del escaneo de vulnerabilidades



Fuente: Propiedad de los autores

3. Posteriormente guardamos la información del escaneo y luego iniciamos el escaneo, ilustración 18.

Ilustración 20: Ejecución del escaneo de vulnerabilidades con Nessus



Fuente: Propiedad de los autores

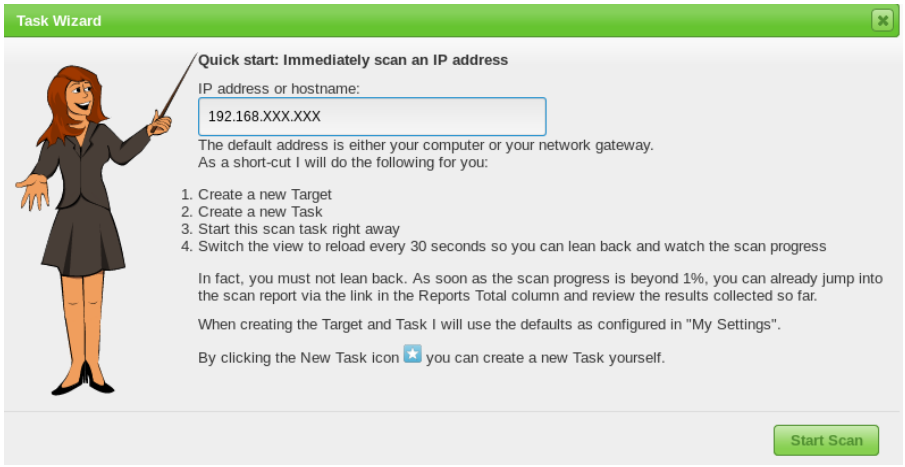
Una vez terminado el escaneo Nessus genero el reporte de las vulnerabilidades encontradas en el servidor, el cual será insumo indispensable para la ejecución de la fase 2 del proyecto.

3.4.1.2. Escaneo de vulnerabilidades con OpenVAS

Como es posible apreciar en las ilustraciones 19, 20 y 21 para la identificación de las vulnerabilidades del servidor con la OpenVAS se siguieron los siguientes pasos:

1. Se creó un nuevo objetivo en el cual se ingresó la dirección IP del servidor del cual se desea identificar las vulnerabilidades que posiblemente este posea.

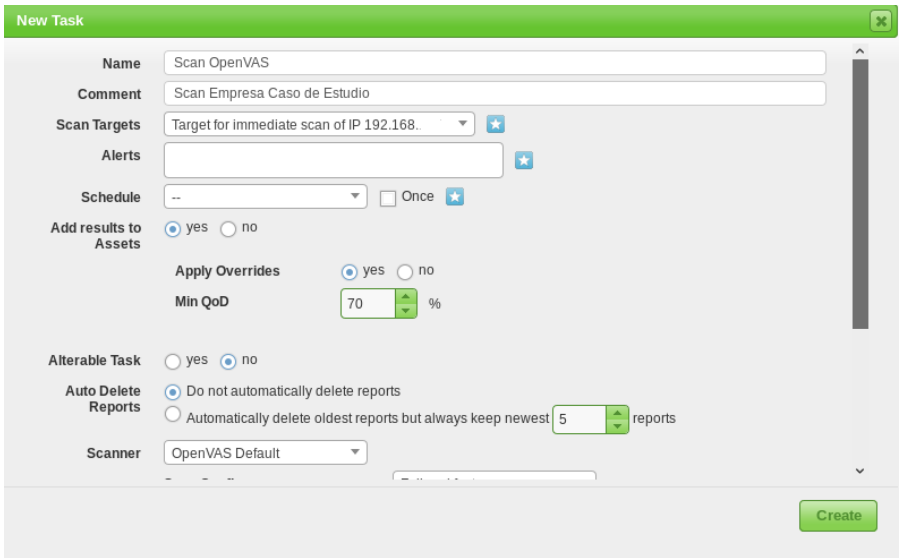
Ilustración 21 Creación de nuevo objetivo en OpenVAS



Fuente: Propiedad de los autores

2. Posteriormente fue necesario configurar una nueva tarea para realizar el escaneo de las vulnerabilidades, se asignó como nombre de esta tarea “Scan OpenVAS” y se procedió a ejecutarlo, tal como se evidencia en la siguiente ilustración.

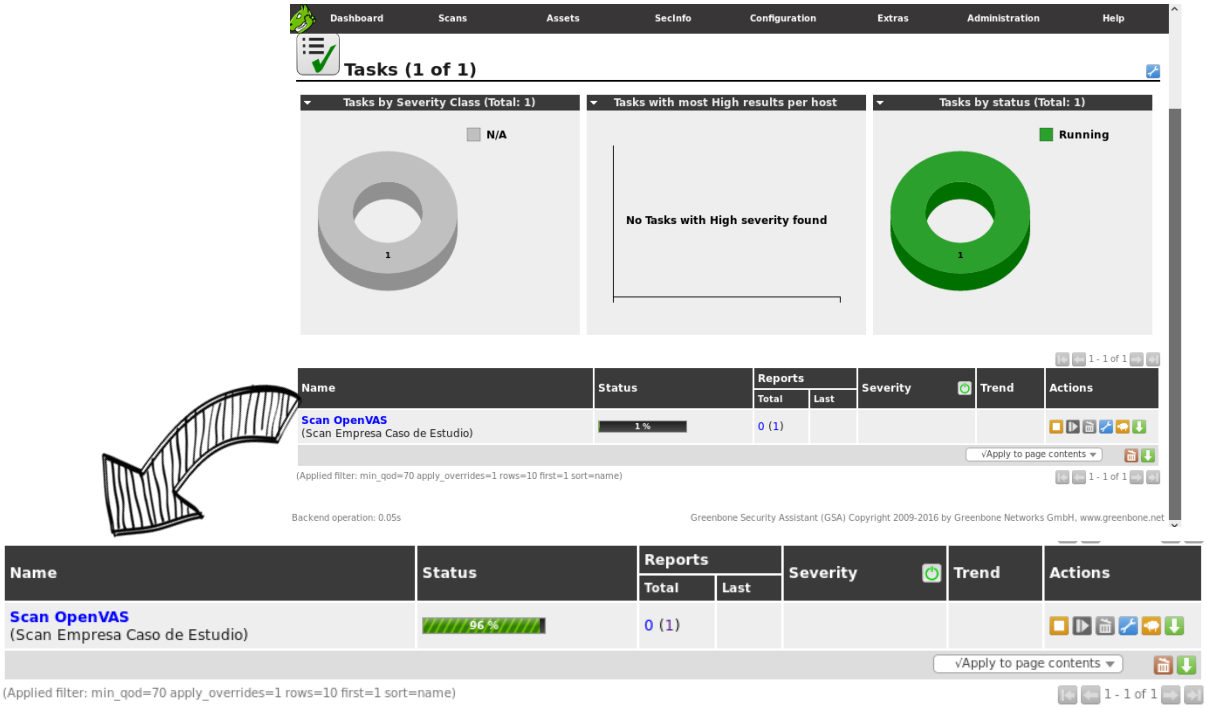
Ilustración 22 Creación tarea de escaneo en OpenVAS



Fuente: Propiedad de los autores

3. Una vez configurada la tarea, se procedió a ejecutar el escaneo de vulnerabilidades.

Ilustración 23 Ejecución del escaneo de vulnerabilidades con Openvas



Fuente: Propiedad de los autores

3.4.1.3. Escaneo de vulnerabilidades con NMAP

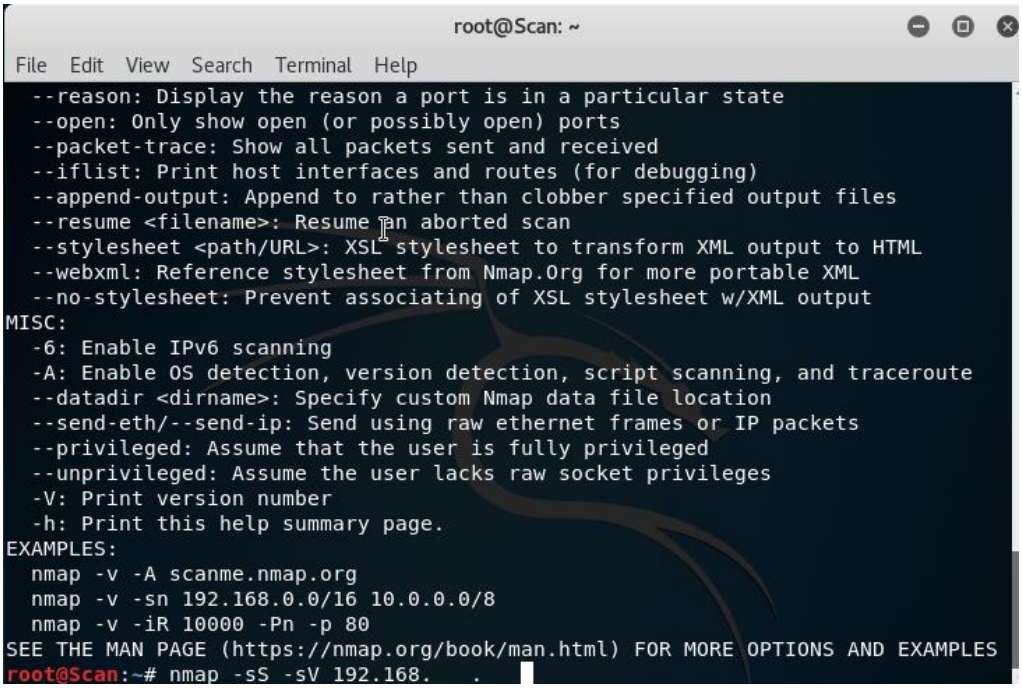
Nmap es una herramienta de código abierto se encuentra preinstala en el sistema operativo Kali Linux, esta herramienta sirve para evaluar la seguridad de los sistemas de información e identificar los servicios implementadas en un servidor de cualquier red informática.

Teniendo en cuenta que es muy peligroso tener puertos abiertos sin ningún servicio corriendo en este, se realizó un escaneo con dicha herramienta que permitió la identificación de los puertos y servicios activos en el servidor principal de la empresa caso de estudio, la información obtenida producto de este escaneo es de vital importancia para la correcta administración y mitigación de vulnerabilidades que puedan originarse en puertos abiertos sin uso.

- **Escaneo a puertos TCP**

En la ilustración 22 se aprecia que para realizar este análisis se usó el comando nmap –sS –sV 192.168.XXX.XXX el cual realizo un escaneo de los puertos abiertos y cerrados y adicionalmente identifico que servicio se encuentra en ejecución en cada uno de ellos.

Ilustración 24 Escaneo de puertos TCP con Nmap



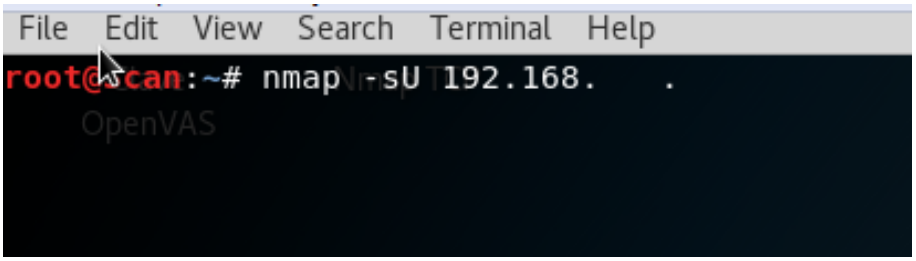
Fuente: Propiedad de los autores

- **Escaneo a puertos UDP**

Si bien la mayoría de servicios de internet usan el protocolo TCP, los protocolos UDP también son muy comunes y a su vez muy vulnerables, los escaneos para la identificación de puertos UDP sin administrar normalmente tardan un tiempo considerable y por esta razón muchos auditores de seguridad tienden a omitirlos cometiendo un grave error, ya que es muy común encontrar servicios UDP muy vulnerables.

Para identificación de los puertos UDP sin administrar y los servicios que se encuentran en ejecución en cada uno de ellos, se usó el comando nmap –sU 192.168.XXX.XXX, tal como se aprecia en la ilustración 23.

Ilustración 25 Escaneo de puertos UDP con Nmap



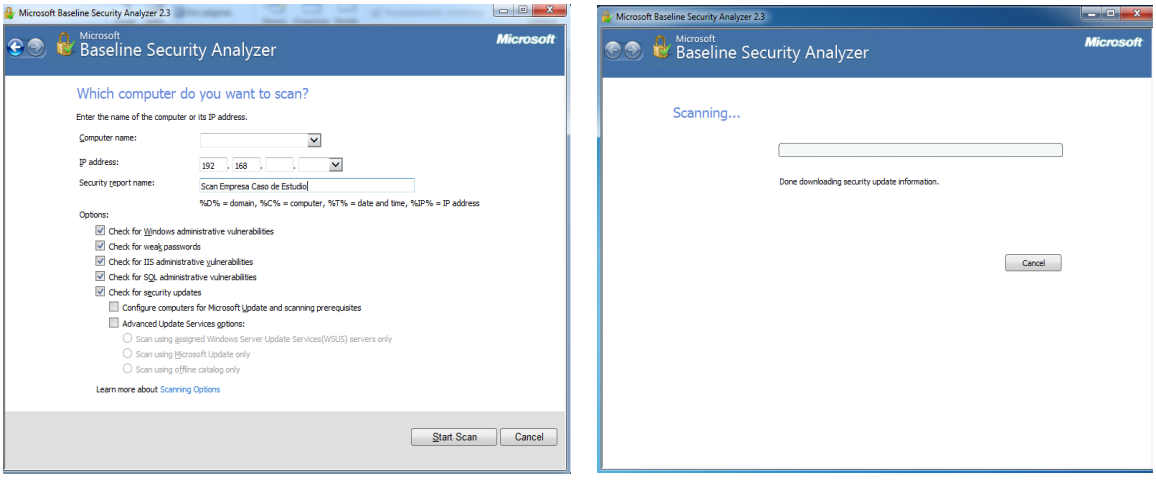
Fuente: Propiedad de los autores

3.4.1.4. Escaneo de vulnerabilidades con Microsoft Baseline Security Analyzer 2.3 (para profesionales de TI)

Microsoft Baseline Security Analyzer proporciona un método optimizado para identificar las actualizaciones de seguridad faltantes y las configuraciones incorrectas de seguridad comunes en el sistema operativo Windows Server 2012 y Windows Server 2012 R2.

Para la realización del análisis con esta herramienta tan solo fue necesario ingresar la dirección IP del servidor previamente virtualizado en VirtualBox y asignar, es posible apreciar esto en la ilustración 24; la herramienta ejecuto automáticamente en análisis y posteriormente se generó el reporte de las vulnerabilidades. Este proceso se puede evidenciar en la siguiente ilustración.

Ilustración 26 Ejecución del escaneo de vulnerabilidades con Microsoft Baseline Security Analyzer



Fuente: Propiedad de los autores

3.4.2. Vulnerabilidades halladas

3.4.2.1. Vulnerabilidades halladas con Nessus Vulnerability Scanner

Una vez realizada la prueba para la identificación de las vulnerabilidades usando la herramienta Nessus Vulnerability Scanner, se obtuvo el reporte arrojado por la aplicación, el cual será uno de los insumos para la evaluación de las vulnerabilidades halladas; las vulnerabilidades están clasificadas como críticas, altas, medias, bajas e informativas, estas últimas no constituyen un factor de riesgo por tanto no serán objeto de evaluación.

En el anexo A se evidencia que el escaneo de vulnerabilidades con Nessus arrojo un total de 82 vulnerabilidades, de las cuales el 5% correspondiente a 4, se clasificaron como riesgo crítico, 17% correspondiente a 14 como riesgo medio, 4% correspondiente a 3 como riesgo bajo y el 75% restante corresponden a 61 vulnerabilidades informativas que no representan factor de riesgo alguno.

3.4.2.2. Vulnerabilidades halladas con OpenVAS

Una vez realizado el escaneo de vulnerabilidades usando la herramienta Open VAS, se obtuvo el reporte arrojado por la aplicación, el cual se aprecia en las ilustraciones 25 a la 44, este será uno de los insumos para la evaluación de las vulnerabilidades halladas; OpenVAS clasifica las vulnerabilidades como altas, medias y bajas.

En el Anexo B se evidencia que el escaneo arrojo un total de 2 vulnerabilidades, las cuales fueron clasificadas como riesgo medio.

3.4.2.3. Vulnerabilidades halladas con NMAP

Con el fin de identificar vulnerabilidades relacionadas con los puertos TCP y UDP y los servicios ejecutados en estos, se usó la herramienta NMAP, la cual permite, a través de sencillos comandos escanear todos los puertos en el servidor y así identificar si existe algún riesgo derivados de una administración ineficiente de los mismos.

- **Escaneo a puertos TCP**

En el Anexo C es posible apreciar que Nmap identifico 17 puertos TCP abiertos y 983 puertos TCP cerrados, sin embargo todos los puertos abiertos tienen un

servicio activo, por tanto no constituyen un riesgo; el resumen de los puertos ser evidencia en la siguiente tabla.

Tabla 4 Resumen escaneo puertos TCP con NMAP

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
80/tcp	open	http	Microsoft IIS httpd 8.5
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2017-11-16 14:42:47Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: XXXXXXXXXXXX.loc, Site: XXX-XXXXX)
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: XXX-XXXXX)
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: XXXXXXXXXXXX.loc, Site: XXX-XXXXX)
3269/tcp	open	tcpwrapped	
3389/tcp	open	ssl	Microsoft SChannel TLS
14000/tcp	open	scotty-ft?	
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC

Fuente: Reporte escaneo a puertos TCP con NMAP

- **Escaneo a puertos TCP**

En el Anexo D es posible apreciar que Nmap identifico 29 puertos UDP abiertos, de los cuales tan solo 3 tienen un servicio en ejecución, los 26 puertos restantes no tienen un servicio activo, por tanto constituyen un riesgo para la seguridad de la información; el resumen de los puertos ser evidencia en la siguiente tabla.

Tabla 5 Resumen escaneo puertos UDP con NMAP

PORT	STATE	SERVICE
123/udp	Open	ntp
137/udp	Open	netbios-ns
389/udp	Open	ldap
49160/udp	Open	unknown
49169/udp	Open	unknown
49171/udp	Open	unknown
49172/udp	Open	unknown
49173/udp	Open	unknown
49174/udp	Open	unknown
49175/udp	Open	unknown
49176/udp	Open	unknown
49177/udp	Open	unknown
49185/udp	Open	unknown
49186/udp	Open	unknown
49193/udp	Open	unknown
49196/udp	Open	unknown
49197/udp	Open	unknown
49198/udp	Open	unknown
49200/udp	Open	unknown
49202/udp	Open	unknown
49205/udp	Open	unknown
49209/udp	Open	unknown
49210/udp	Open	unknown
49222/udp	Open	unknown
49226/udp	Open	unknown
49306/udp	Open	unknown
49393/udp	Open	unknown
64513/udp	Open	unknown
64590/udp	Open	unknown

Fuente: Reporte escaneo a puertos UDP con NMAP

3.4.2.4. Vulnerabilidades halladas con Microsoft Baseline Security Analyzer

Como es posible apreciar en el Anexo E una vez realizado el escaneo de vulnerabilidades usando la Microsoft Baseline Security Analyzer se logró identificar un total de 9 vulnerabilidades las cueles están clasificadas como altas, medias y bajas. Es importante aclarar que por limitaciones consecuentes al acuerdo de vulnerabilidad se omitieron o censuraron algunas hojas del reporte.

4. EVALUACION DE LAS VULNERABILIDADES DEL SERVIDOR PRINCIPAL

4.1. ANÁLISIS DE LOS REPORTE DE ESCANEO DE VULNERABILIDADES

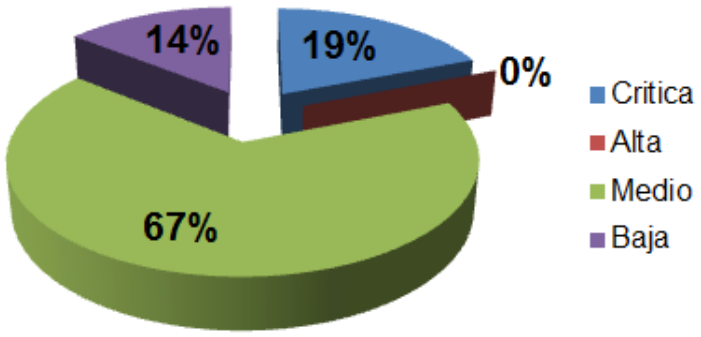
4.1.1. Análisis reporte del escaneo de vulnerabilidades Nessus

Una vez realizada la prueba para la identificación de las vulnerabilidades usando la herramienta Nessus Vulnerability Scanner, procedemos al análisis de las vulnerabilidades halladas, las cuales la aplicación clasifica como críticas, altas, medias, bajas e informativas, estas últimas no constituyen un factor de riesgo por tanto no serán objeto de evaluación.

Como es posible apreciar en la ilustración 51 el escaneo de vulnerabilidades arrojo un total de 21 vulnerabilidades, de las cuales el 19% correspondiente a 4, se clasificaron como riesgo crítico, 67% correspondiente a 14 como riesgo medio y 14% correspondiente a 3 como riesgo bajo.

Ilustración 27 Resumen de vulnerabilidades Nessus

Vulnerabilidades	
Riesgo	**Cantidad**
Critica	4
Alta	0
Medio	14
Baja	3
Total	**21**



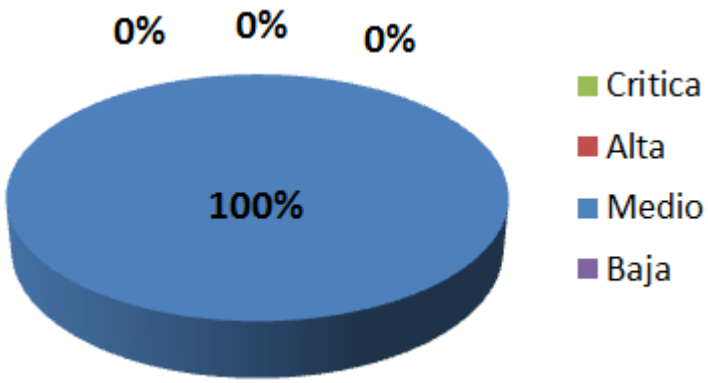
Fuente: Reporte escaneo de vulnerabilidades Nessus

4.1.2. Análisis reporte del escaneo de vulnerabilidades OpenVAS

Con el fin de corroborar los hallazgo obtenidos con la herramienta Nessus, se realizo un escaneo de vulnerabilidades con OpenVAS, la ilustración 52 ilustra el resultado de dicho escaneo, el cual, solo arrojo 2 vulnerabilidades las cueles fueron clasificadas con factor de riesgo medio.

Ilustración 28 Resumen de vulnerabilidades OpenVAS

Vulnerabilidades	
Riesgo	**Cantidad**
Critica	0
Alta	0
Medio	2
Baja	0
Total	**2**



Fuente: Reporte escaneo de vulnerabilidades OpenVAS

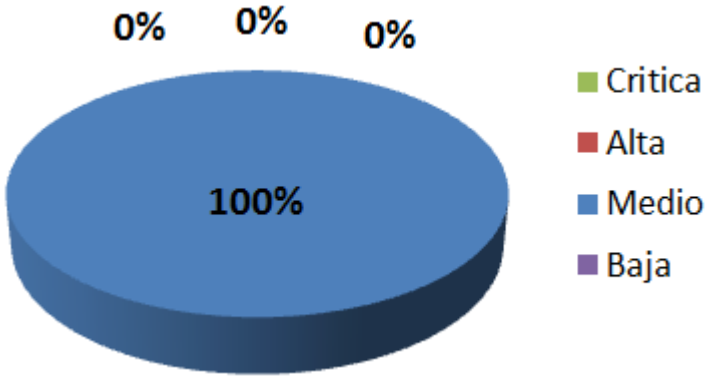
4.1.3. Análisis reporte del escaneo de vulnerabilidades NMAP

Con el fin de identificar vulnerabilidades relacionadas con los puertos TCP y UDP y los servicios ejecutados en estos, se usó la herramienta NMAP, la cual permite, a través de sencillos comandos escanear todos los puertos en el servidor y así identificar si existe algún riesgo derivados de una administración ineficiente de los mismos.

La ilustración 53 se aprecia que solo fue detectada una vulnerabilidad relacionada con la administración de los puestos UDP del servidor, la cual representa un riesgo medio para la seguridad informática de la empresa caso de estudio.

Ilustración 29 Resumen de vulnerabilidades NMAP

Vulnerabilidades	
Riesgo	**Cantidad**
Critica	0
Alta	0
Medio	1
Baja	0
Total	**1**



Fuente: Reporte escaneo de vulnerabilidades NMAP

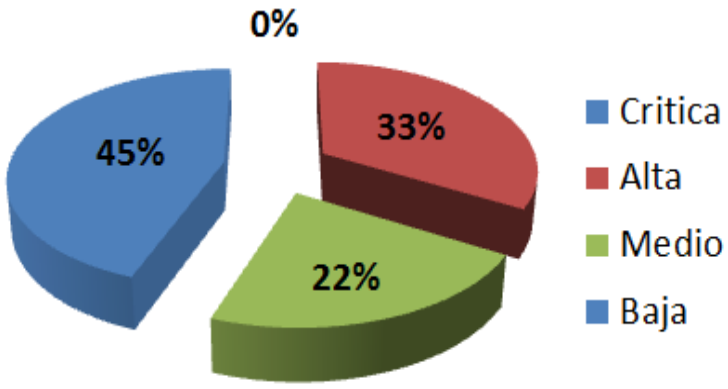
4.1.4. Análisis reporte del escaneo de vulnerabilidades Microsoft Baseline Security Analyzer

En la ilustración 54 se aprecia que una vez realizado el escaneo de vulnerabilidades usando la Microsoft Baseline Security Analyzer se logró identificar un total de 9 vulnerabilidades las cueles están clasificadas como altas, medias y bajas. Es importante aclarar que por limitaciones consecuentes al acuerdo de vulnerabilidad se omitieron o censuraron algunas hojas del reporte.

Como es posible apreciar en la ilustración 54 el escaneo de vulnerabilidades realizado con Microsoft Baseline Security Analyzer arrojo un total de 9 vulnerabilidades, de las cuales el 33% correspondiente a 3, se clasificaron como riesgo crítico, 22% correspondiente a 2 como riesgo medio y 45% correspondiente a 4 como riesgo bajo.

Ilustración 30 Resumen de vulnerabilidades Microsoft Baseline Security Analyzer

Vulnerabilidades	
Riesgo	**Cantidad**
Critica	0
Alta	3
Medio	2
Baja	4
Total	**9**



Fuente: Reporte escaneo de vulnerabilidades Microsoft Baseline Security Analyzer

4.1.5. Consolidad de los escaneos de vulnerabilidades

Realizadas las pruebas para la identificación de las vulnerabilidades usando las herramientas Nessus, OpenVAS, NMAP y Microsoft Baseline Security Analyzer se realizó a la evaluación de las vulnerabilidades halladas, las cuales, están clasificadas como críticas, altas, medias y bajas. El escaneo de vulnerabilidades arrojo un total de 33 vulnerabilidades, de las cuales el 12% correspondiente a 4 vulnerabilidades se clasificaron como riesgo crítico, 9% correspondiente a 3 como riesgo alto, 58% correspondiente a 19 como riesgo medio y el 21% restante

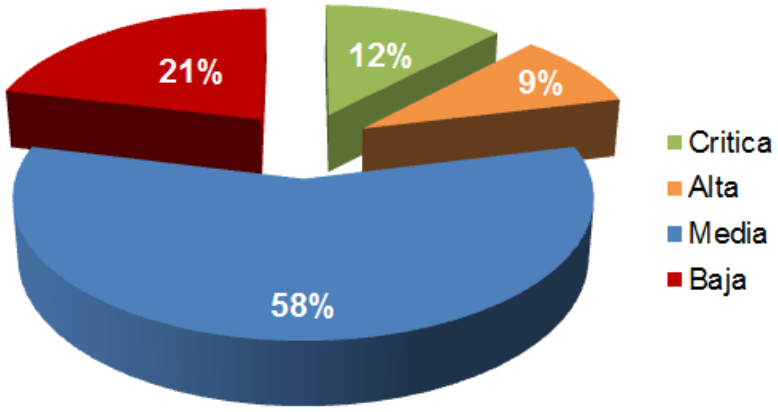
corresponden a 7 vulnerabilidades clasificadas con riego bajo. Esto se puede ilustrar mejor en la siguiente tabla y gráfico.

Tabla 6 Resumen de las vulnerabilidades

Vulnerabilidades					
Nivel de riesgo	**Nessus**	**OpenVAS**	**NMAP**	**Microsoft Baseline Security Analyzer**	**Total Vulnerabilidades**
Critica	4	0	0	0	**4**
Alta	0	0	0	3	**3**
Medio	14	2	1	2	**19**
Baja	3	0	0	4	**7**
Total	**21**	**2**	**1**	**9**	**33**

Fuente: Propiedad de los autores

Ilustración 31: Resumen de vulnerabilidades Nessus



Fuente: Propiedad de los autores

4.2. VULNERABILIDADES DE RIESGO CRÍTICO

Se identificaron 4 vulnerabilidades críticas, las cuales serán descritas y analizadas, y se planteara una solución para la mitigación del riesgo que representa cada una de ellas.

4.2.1. Vulnerabilidad en http.sys - ejecución remota de código

Esta vulnerabilidad es causada por una condición de desbordamiento de enteros en el protocolo HTTP (HTTP.sys) debido

.

Al análisis incorrecto de las solicitudes HTTP hechas. Esta vulnerabilidad podría permitir la ejecución de un código malicioso con privilegios del sistema por un atacante remoto no autenticado.

4.2.2. Vulnerabilidades múltiples de Microsoft Windows SMBV1

El host remoto de Windows Microsoft Server Message Block 1.0 (SMBv1) se encuentra habilitado. Por lo tanto, está afectado por múltiples vulnerabilidades las cuales hacen que en Microsoft Server Message Block 1.0 (SMBv1) divulgue información a causa del manejo incorrecto de paquetes y solicitudes SMBv1, esto puede permitirle a una persona no autorizada explotar estas vulnerabilidades mediante paquetes SMBv1 y /o solicitudes SMB especialmente diseñadas, lo cual haría que el sistema deja de responder.

4.2.3. Vulnerabilidad en schannel - ejecución remota de código malicioso

Esta vulnerabilidad se genera a causa del procesamiento incorrecto de paquetes por el Secure Channel (Schannel), lo cual permite que una persona pueda explotar este problema enviando paquetes especialmente diseñados a al servidor. Es importante tener en cuenta que este protocolo realiza un envío a través del protocolo TLS que le permite confirmar la identidad de un cliente el cual es seguido por un mensaje CertificateVerify. Algunos hosts cierran la conexión cuando reciben un certificado de cliente para el que no se solicitó un mensaje CertificateReques, a causa de esto no es posible en algunas ocasiones detectar esta vulnerabilidad.

4.2.4. Vulnerabilidad de seguridad en el servidor SMB de Microsoft Windows (Eternalchampion) (Eternalromance) (Eternalsynergy) (Wannacry) (Eternalrocks) (Petya)

El servidor remoto de Windows está afectado por diversas vulnerabilidades ocasionadas el manejo inadecuado de solicitudes en la ejecución remota de código y divulgación de información en Microsoft Server Message Block 1.0 (SMBv1).

Esto podría permitirle a un atacante remoto la explotación de estas vulnerabilidades a través de un paquete especialmente diseñado, para ejecutar código malicioso o de un paquete especialmente diseñado, para revelar información confidencial

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y explotaciones del Grupo de Ecuaciones reveladas el 2017/04/14 por un grupo conocido como los Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que utiliza por primera vez CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

4.2.5. Vulnerabilidades múltiples de ejecución remota de código de Windows SMB

Se presentan distintas vulnerabilidades, que se originan en la manera en que un servidor Microsoft Server Message Block 1.0 (SMBv1) realiza su ejecución remota de código y gestiona algunas solicitudes. Dado el caso si un tercero no autorizada logra sacar beneficio de dichas vulnerabilidades, podrá ejecutar comandos en el servidor de destino, poniendo en riesgo la estabilidad y confiabilidad de los sistemas informáticos. ¿Cómo lo realiza?, el atacante envía un paquete de código al servidor SMBv1 de destino, sin necesidad de ser un usuario autenticado.

Una actualización de seguridad hace frente a estas vulnerabilidades, donde se realiza la corrección de como el servidor SMBv1 hace la gestión de todo tipo de solicitud, especialmente las diseñadas con un objetivo especial.

A continuación, se presenta la Tabla 6, la cual indica los enlaces a la entrada de las vulnerabilidades y sus exposiciones más comunes.

Tabla 7: lista de vulnerabilidades y exposiciones comunes de ejecución remota de código de Windows SMB

Vulnerabilidad	Numero CVE	Revelada públicamente	Explotada
Vulnerabilidad de ejecución remota de código de Windows SMB	CVE-2017-0143	No	No
Vulnerabilidad de ejecución remota de código de Windows SMB	CVE-2017-0144	No	No
Vulnerabilidad de ejecución remota de código de Windows SMB	CVE-2017-0145	No	No
Vulnerabilidad de ejecución remota de código de Windows SMB	CVE-2017-0146	No	No
Vulnerabilidad de ejecución remota de código de Windows SMB	CVE-2017-0148	No	No

Fuente: Boletín de seguridad de Microsoft MS17-010

En caso de no aplicarse la actualización se recomienda que los usuarios interrumpan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede deshabilitar siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos fronterizos de la red.

4.2.6. Vulnerabilidad de divulgación de información de Windows SMB

Esta vulnerabilidad se produce a causa de la posibilidad de envió de códigos por parte del atacante donde se logra controlar el servidor Microsoft Server Message Block 1.0 SMBv1 sin necesidad de estar autenticado; debido a que este controla erróneamente algunas solicitudes. La solución se da al realizar una actualización de seguridad. A continuación, se presenta la Tabla 8, la cual indica los enlaces a la entrada de las vulnerabilidades y sus exposiciones más comunes.

Tabla 8: lista de vulnerabilidades y exposiciones comunes de divulgación de información de Windows SMB

Vulnerabilidad	Numero CVE	Revelada públicamente	Explotada
Vulnerabilidad de divulgación de información de Windows SMB	CVE-2017-0147	No	No

Fuente: Boletín de seguridad de Microsoft MS17-010

4.3. VULNERABILIDADES DE RIESGO ALTO

4.3.1. Actualizaciones de seguridad, paquetes acumulativos de actualizaciones y Service Packs

El análisis de vulnerabilidad comprobó que existen actualizaciones disponibles que no están instaladas en el servidor. Las actualizaciones que se escanean en busca de seguridad se dividen en tres categorías relacionadas con el ciclo de vida de una solución de seguridad.

Las actualizaciones de seguridad son actualizaciones relacionadas con la seguridad que generalmente abordan un error específico o vulnerabilidad de seguridad. Todas las actualizaciones de seguridad que se ofrecen durante la vida útil de un paquete de servicio se combinan en el siguiente service pack. Cada

actualización de seguridad identificada por esta herramienta tiene un boletín de seguridad de Microsoft asociado que contiene más información sobre la corrección.

Los paquetes acumulativos de actualizaciones son un conjunto acumulativo de soluciones de seguridad. Estas actualizaciones se publican periódicamente y, debido a que son más pequeñas que los paquetes de servicio completo, tienden a ser más fáciles de implementar. Como los paquetes acumulativos de actualizaciones se centran en problemas de seguridad, también tienden a ser más fáciles de implementar que las actualizaciones de seguridad múltiples. Por ejemplo, al actualizar una computadora que se ha instalado recientemente y puede que no tenga actualizaciones de seguridad que la protejan.

Los Service Packs son colecciones de actualizaciones de seguridad y no de seguridad que se centran en una variedad de mejoras y soluciones para un producto de Microsoft. Los Service Packs proporcionan soluciones para problemas que se han notificado después de que el producto se haya vuelto disponible en general. Los paquetes de servicio son acumulativos, lo que significa que cada paquete de servicio nuevo contendrá todas las correcciones de los paquetes de servicios anteriores, además de las nuevas correcciones. Están diseñados para garantizar la compatibilidad de la plataforma con el software y los controladores recién lanzados, y contienen actualizaciones que solucionan problemas descubiertos por los clientes o mediante pruebas internas.

Cuando el servidor ejecuta los paquetes de servicio más recientes y los últimos paquetes acumulativos de actualizaciones, puede minimizar la cantidad de actualizaciones de seguridad individuales adicionales que se necesitan y mitigar los riesgo generados al no instalarlos.

4.3.2. SQL Server se ejecuta en el controlador de dominio

Esta comprobación determino que Microsoft SQL Server se ejecuta en el sistema el cual es un controlador de dominio.

Los controladores de dominio contienen datos confidenciales, como la información de la cuenta de usuario, y no deben utilizarse en otra función. Si ejecuta una base de datos de SQL Server en un controlador de dominio, aumenta la complejidad involucrada en la seguridad del servidor y la protección contra ataques.

4.3.3. Las zonas de Internet Explorer no tienen configuraciones seguras para algunos usuarios.

Se compruebo que la configuración de seguridad actual para las zonas de Internet Explorer en cada usuario local del servidor. Las zonas que no utilizan la configuración recomendada para algunos usuarios tal como se evidencia en la siguiente tabla.

Tabla 9 Usuarios con configuraciones no seguras en Internet Explorer

Usuarios	Zona	Configuración	Selección
XXX\williams.avila	Internet	Descargar los controles firmados de ActiveX	Predeterminado
	Internet	Descargar de archivo	Habilitado
	Internet	Enviar datos de formulario no encriptados	Habilitado

Fuente: Propiedad de los autores

Las zonas de contenido web de Microsoft Internet Explorer dividen Internet o Intranet en zonas con diferentes niveles de seguridad. Esta capacidad le permite establecer configuraciones globales predeterminadas para el navegador, permitir todo el contenido en sitios confiables o rechazar ciertos tipos de contenido, como los applets de Java o los controles ActiveX, según el sitio web de origen.

El software de exploración de Internet Explorer incluye cuatro zonas de contenido web predefinidas: Internet, intranet local, sitios de confianza y sitios restringidos. En el cuadro de diálogo Opciones de Internet, puede establecer las opciones de seguridad que desee para cada zona y luego agregar o eliminar sitios de cualquier zona (excepto Internet), dependiendo de su nivel de confianza en el sitio. En entornos corporativos, los administradores pueden configurar zonas para los usuarios. También pueden agregar o eliminar (por adelantado) los certificados de autenticación de los editores de software en los que confían o no, para que los usuarios no tengan que tomar decisiones de seguridad mientras usan Internet.

Para cada zona de seguridad, puede elegir una configuración de seguridad alta, mediana, media baja, baja o personalizada. La configuración alta se recomienda para sitios en zonas de confiabilidad incierta. La opción personalizada proporciona a los usuarios y administradores avanzados más control sobre todas las opciones de seguridad, incluidas las siguientes:

- Acceso a archivos, controles ActiveX y scripts.
- Nivel de capacidades otorgadas a los applets de Java.
- Designación de identidad del sitio con autenticación Secure Sockets Layer (SSL).

- Protección de contraseña con autenticación NTLM. (Dependiendo de en qué zona esté el servidor, Internet Explorer puede enviar información de contraseña automáticamente, solicitar al usuario información de usuario y contraseña, o denegar cualquier solicitud de inicio de sesión).

En los sistemas que tienen instalada la configuración de seguridad mejorada de Internet Explorer, la configuración se compara con los niveles recomendados por defecto para esta configuración.

4.4. VULNERABILIDADES DE RIESGO MEDIO

4.4.1. Vulnerabilidad de seguridad para los protocolos remotos SAM Y LSAD (3148527) (BADLOCK)

Esta vulnerabilidad en el Security Account Manager SAM permite a un atacante interceptar la comunicación entre el cliente y el servidor que aloja datos del Security Account Manager SAM, y explotar esta vulnerabilidad, buscando violar el nivel de autenticación de credenciales de acceso, de esta manera se suplanta algún usuario que posee los permisos necesarios para acceder a la base de datos SAM. Esto se presenta cuando el host remoto de Windows es afectado por una vulnerabilidad, la cual permite la elevación de privilegios en el protocolo SAM y en la Autoridad de Seguridad Local LSAD, producto de una validación incorrecta en el Remote Procedure Call RPC.

4.4.2. El certificado SSL no confiable

Esta vulnerabilidad se evidencia cuando se puede romper la cadena de confianza y no se puede confiar en el certificado X.509 del servidor. Se da por tres posibles eventos:

- Cuando la primera parte de la cadena de un certificado auto firmado no conocido o cuando hacen falta certificados que intercedan y hagan la conexión en la parte superior de la cadena de certificados en una autoridad pública de certificación.
- En el momento en que la cadena de certificados contiene un certificado no valido en su fase de exploración. Se presenta al momento de que el análisis se da antes de las fechas 'notBefore' del certificado o después de que se da la fecha uno de los certificados 'notAfter'

- Finalmente cuando la cadena de certificados contiene una firma que puede contener una firma que no corresponde a los datos del certificado o que la firma no pudo ser comprobada. Las firmas malas pueden ser fijadas consiguiendo el certificado con la mala firma para ser re-firmado por su emisor.

4.4.3. certificado SSL con nombre de host incorrecto

El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.

4.4.4. Certificado SSL auto-firmado

Al no estar firmada por una autoridad certificada la cadena de certificados X.509, da el lugar a que si el host remoto es público, esto hace que no requiera el uso de SSL, con esto cualquiera puede ejecutar un ataque Man in the Middle hacia el host. Es importante tener presente que estos complementos no realizan la comprobación de las cadenas de certificados que finalizan en un certificado que no está auto firmado y a su vez está firmado por una autoridad no conocida.

4.4.5. Caché de servidores DNS - detección de información remota

Un servidor DNS remoto da respuesta a cada consulta realizada por dominios de terceros que no contienen el bit de recursión definido. Esta situación hace posible que un tercero no autorizado de manera remota determine los dominios que se han accedido últimamente por medio del servidor de nombre, por lo tanto, saber los host navegados recientemente. En el caso de un DNS interno que no tiene acceso a la red externa, un ataque tendría un alcance solamente dentro de la red interna.

4.4.6. Vulnerabilidad en el servidor de protocolo de escritorio remoto de Microsoft Windows Man-In-The-Middle Weakness

En este caso se evidencia un riesgo en el Protocolo de Escritorio Remoto de Microsoft Windows, ya que, la versión utilizada del Servidor de Protocolo de Escritorio Remoto es un agente vulnerable a un ataque Man in the Middle, cuando el cliente RDP no valida la identidad del servidor en la configuración del cifrado. Aquí un tercero no autorizado tiene la posibilidad de hacer una interceptación en el tráfico desde el servidor RDP donde se puede dar un cifrado entre el cliente y el servidor sin ser detectado. El ataque perpetrado permite al delincuente informático

saber cualquier dato confidencial de una red. Esta falla se da porque el servidor RDP guarda una clave privada RSA codificada en la biblioteca mstlsapi.dll. Todo usuario local con acceso a este fichero (en cualquier sistema Windows) puede tomar las credenciales y emplear para cualquier fin.

4.4.7. Microsoft Windows SMB lsaquery information policy función enumeración SID sin credenciales

Al emular la llamada a LsaQueryInformationPolicy (), fue posible obtener el SID del host (Identificador de seguridad), sin credenciales.
El valor SID del host remoto es: 1-5-21-335902862-598095521-666385194

La comprobación SSR determina si la configuración del Registro RestrictAnonymous se utiliza para restringir las conexiones anónimas en el equipo escaneado. La configuración del registro está en la ubicación siguiente:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous

Los usuarios anónimos pueden enumerar ciertos tipos de información del sistema, incluidos los nombres de usuario y los detalles, las políticas de cuentas y los nombres compartidos. La lista de nombres de usuario y nombres compartidos podría ayudar a los atacantes potenciales a obtener información comprometedora, como por ejemplo:

- Quién es un administrador.
- Qué equipos cuentan con protección de cuenta débil.
- Qué equipos comparten información con la red.

4.4.8. Firma SMB deshabilitada

Esta vulnerabilidad se genera al no ser necesaria la firma en el servidor SMB remoto, se presenta la posibilidad para un atacante informático de realizar un ataque Man in the Middle.

El protocolo SMB proporciona la base para el intercambio de archivos e impresoras de Microsoft y muchas otras operaciones de red, como la administración remota de Windows. Para ayudar a prevenir ataques que modifican paquetes SMB en tránsito, el protocolo SMB admite la firma digital de paquetes SMB. Esta configuración de directiva determina si se debe negociar la firma de paquetes SMB antes de que se permita la comunicación con un cliente SMB.

Si esta configuración está habilitada, el servidor de red de Microsoft no se comunicará con un cliente de red de Microsoft a menos que el cliente acepte realizar la firma de paquetes SMB.[53]

4.4.9. SMB utiliza host SID para enumerar usuarios locales sin credenciales

Esta vulnerabilidad se genera a causa de una falla en el sistema remoto de Windows, el cual permite que un atacante tenga la posibilidad identificar sin credenciales, los usuarios locales que alguna vez ha tomado el servidor remotamente, esto es posible usando en identificador de seguridad del host (SID).

Esta es una vulnerabilidad común en los sistemas operativos Windows relacionada con la gestión de usuarios y puede llevar a que un atacante que loge penetrar en la red realice un ataque de fuerza bruta con diccionario para hallar la clave de acceso de uno de los usuarios identificados, para lo cual hay desenas de exploits disponibles.

4.4.10. Suites de cifrado de tamaño de bloque SSL de 64 bits admitidas (SWEET32)

Esta vulnerabilidad se crea ya que el puerto y usado para la conexión remota permite el uso de bloques cifrados de 64 bits, esta vulnerabilidad es normalmente conocida como SWEET32, debido a que los bloques cifrados a 64 bits son débiles, una persona no autorizada puede usar un ataque Man In the Middle y con los recursos y herramientas idóneos podría explotar esta vulnerabilidad, con esto es posible que el atacante pueda obtener cookies, HTTPS seguras y posiblemente el secuestro y suplantación de una sesión legitimada, todo es, el atacante puede lograrlo en tan solo 30 horas.

4.4.10.1. Lista de suites de cifrado de bloque de 64 bits admitidas por el servidor remoto:

Cifras de intensidad media (> 64 bits y <clave de 112 bits o 3DES)
DES-CBC3-SHA Kx = RSA Au = RSA Enc = 3DES-CBC (168) Mac = SHA1

Los campos de arriba son:

{OpenSSL ciphername}
Kx = {intercambio de claves}yk
Au = {autenticación}

[53] Protocolo SMB basado en https://msdn.microsoft.com/es-es/library/hh831795(v=ws.11).aspx

Enc = {método de cifrado simétrico}
Mac = {código de autenticación de mensaje} {bandera de exportación}

4.4.11. Certificado SSL firmado utilizando algoritmo de HASH débil

Esta vulnerabilidad es ocasionada debido a que los siguientes certificados usan un algoritmo de hashing débil criptográficamente, tales como MD2, MD4, MD5 o SHA1:

| -Subject: CN = XXXXX. XXXXXXXXXXXXX.loc
| -Algoritmo de firma: SHA-1 con cifrado RSA
| -Valida de: 13 de mayo 00:01:31 GMT 2017
| -Válido a: 12 de noviembre 00:01:31 GMT 2017

Al usar algoritmos débiles estos certificados son especialmente vulnerables a los ataques de colisión. Al explotar esta vulnerabilidad una persona no autorizada podría crear otro certificado con la misma firma digital, lo que permite que un atacante se haga pasar por el servicio comprometido o afectado.

4.4.12. Soporte de cifrado SSL de mediana intensidad

Esta vulnerabilidad es causada por la admisión de cifrados SSL con cifrados clasificados como de fuerza media, es decir aquellos que usan entre 64 bits hasta 112 bits o cifrado 3DES. Esto permite que un atacante que haya logra penetrar la red física pueda evadir fácilmente este tipo de cifrados.

Teniendo en cuenta la posibilidad de ejecutar JavaScript en un navegador de internet, una persona no autorizada dentro de la red física puede generar el tráfico suficiente para obtener una colisión que le permita capturar información tales como cookies y así hacerse a una sesión de un usuario legítimo.

A continuación se lista los cifrados SSL de fuerza media admitidos por el servidor remoto con cifras de intensidad media (> 64 bits y <clave de 112 bits o 3DES)
DES-CBC3-SHA Kx = RSA Au = RSA Enc = 3DES-CBC (168) Mac = SHA1

Los campos de arriba son:

{OpenSSL ciphername}
Kx = {intercambio de claves}
Au = {autenticación}
Enc = {método de cifrado simétrico}
Mac = {código de autenticación de mensaje} {bandera de exportación}

4.4.13. Servicios de terminal server no utiliza autenticación de nivel de red (NLA)

Esta vulnerabilidad es causada cuando no están configurados para usar autenticación de nivel de red (NLA) exclusivamente en los Servicios del terminal remoto, NLA usa el protocolo del proveedor de soporte de seguridad de credenciales (CredSSP) para realizar una autenticación de servidor sólida ya sea a través de mecanismos TLS / SSL o Kerberos, que resguardan contra los ataques man-in-the-middle. Además de mejorar la autenticación, NLA también ayuda a proteger la computadora remota de usuarios malintencionados y software al completar la autenticación del usuario antes de establecer una conexión RDP completa.

4.4.14. El nivel de cifrado de servicios de terminal server es medio

Es vulnerabilidad se hace presenta ya que el terminal Server no posee una configuración que le permita usar criptografía fuerte. La terminal está usando actualmente criptografía de nivel medio lo cual podría permitirle a un atacante acceder a las comunicaciones fácilmente y así obtener capturas de pantalla e incluso la posibilidad de enviar comandos ya que tendría la opción de hacer pulsaciones de teclas.

4.4.15. Vulnerabilidad de denegación de servicios TCP/IPv4

Es posible detectar esta vulnerabilidad realizando el envío de un paquete TCP Reset con un número de secuencia diferente al objetivo, luego se verifica una conexión previamente abierta para ver si el objetivo la cerró o no. El error se desencadena cuando la pila TCP objetivo recibe paquetes de reinicio TCP falsificados las cuales dan como resultado la pérdida de disponibilidad para los servicios TCP atacados lo cual significa es propenso a la vulnerabilidad de denegación de servicio.

El Impacto de esta vulnerabilidad radica en la posibilidad de explotación exitosa de la misma, lo cual podría permitir a los atacantes remotos adivinar los números de secuencia y provocar una denegación de servicio a las conexiones TCP persistentes inyectando repetidamente un paquete TCP RST.

Esta vulnerabilidad normalmente es explotada mediante un ataque DoS el cual puede ser llevado a cabo de diversas formas. Aunque básicamente radican en:[54]

[54] Siles Raul, Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Primera Edición, 2002.

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

4.4.16. Vulnerabilidad en los informes de enumeración de servicios de MSRPC

Esta vulnerabilidad surge al ser posible enumerar realizando las consultas apropiadas los servicios MSRPC que se ejecutan en el puerto 135, esta vulnerabilidad permite que un atacante pueda usar este hecho para obtener más información y conocimiento sobre el host remoto y la red.

MSRPC implementa extensiones específicas de Microsoft que históricamente lo han separado de otras implementaciones de RPC. Muchas de estas interfaces han estado en Windows desde su inicio, proporcionando una gran superficie de irrupción para ataques de desbordamiento de búfer y similares. El mapeador de puertos MSRPC se anuncia en TCP y UDP 135 por los sistemas de Windows, y no se puede deshabilitar sin afectar drásticamente la funcionalidad principal del sistema operativo. Las interfaces MSRPC también están disponibles a través de otros puertos, incluidos TCP / UDP 139, 445 o 593, y también pueden configurarse para escuchar a través de un puerto HTTP personalizado a través de IIS o COM Internet Services

4.4.17. Puertos UDP abiertos sin administrar

Si bien la mayoría de servicios de internet usan el protocolo TCP, los protocolos UDP también son muy comunes y a su vez muy vulnerables, los escaneos para la identificación de puertos UDP sin administrar normalmente tardan un tiempo considerable y por esta razón muchos auditores de seguridad tienden a omitirlos cometiendo un grave error, ya que es muy común encontrar servicios UDP muy vulnerables.

Nmap identifico 29 puertos UDP abiertos, de los cuales tan solo 3 tienen un servicio en ejecución, los 26 puertos restantes no tienen un servicio activo, por tanto constituyen un riesgo para la seguridad de la información.

Poseer un puerto abierto es similar a tener una puerta la cual te permite entrar y salir de tu casa, pasa exactamente lo mismo con una computadora con un puerto abierto sin administrar podrás establecer una conexión y entrar y salir de ella, sin embargo un extraño también lo podrá hacer, teniendo la oportunidad de espiar, robar nuestra información y/o dañar el servidor.

Los puertos abiertos sin un servicio activo deben ser cerrados inmediatamente, con el fin de reducir las posibilidades para que un cracker escanee tu sistema, encontrar vulnerabilidades y ejecute un ataque que afecte el servidor.

4.4.18. Cuentas de usuario con contraseñas sin vencimiento.

Se determinó que 630 cuentas de usuario de las 4951 existentes tienen contraseñas sin vencimiento.
Las cuentas de usuario local que poseen una contraseña que no caduca no se mostraron en el reporte del escaneo por motivos de seguridad, sin embargo serán informadas al área encargada de la seguridad informática de la empresa caso de estudio.

4.4.19. Se encontraron más de 2 administradores en el servidor.

La verificación identifico y enumero las cuentas de usuario individuales que pertenecen al grupo de administradores locales. Se detectaron más de dos cuentas de administrador individuales, Microsoft Baseline Security Analyzer listó los nombres de las cuentas y marco el cheque como una posible vulnerabilidad. En general, se recomienda mantener el número de administradores al mínimo, porque los administradores esencialmente tienen control total sobre la computadora.

4.5. VULNERABILIDADES DE RIESGO BAJO

4.5.1. Detección de servidor DHCP

Esta vulnerabilidad se genera cuando el servidor DHCP revela información relacionada al diseño e la red, permitiendo obtener información sensible que podría ser útil para que un atacante se familiarice con la red y así poder planear un ataque que pueda comprometer el servidor, esta información pude ser el NIS, nombre de dominio, la lista de los servidores web de la red, entre otros.

Con el escaneo fue recopilar la siguiente información del servidor DHCP:

- Servidor maestro DHCP de esta red: 192.168.XXX.XXX
- Dirección IP que el servidor DHCP nos atribuiría: 192.168.XXX.69
- Máscara de red: 255.255.XXX.0
- Identificador del servidor DHCP: 192.168.XXX.XXX
- Enrutador: 192.168.XXX.XXX
- Servidor (es) de nombre de dominio: 172.XXX.XXX.XXX, 172. XXX.XXX.XXX
- Nombre de dominio: XXXXXXXXXXXXX.loc

4.5.2. SSL RC4 CIPHER SUITES soportado (BAR MITZVAH)

Esta vulnerabilidad se genera debido a que el puerto 3389/tcp/msrdp admite el uso de RC4 en una o más suites de cifrado. El cifrado RC4 está viciado en su generación de una secuencia pseudoaleatoria de bytes, de modo que se introduce una amplia variedad de pequeños sesgos en la secuencia, disminuyendo su aleatoriedad.

Lista de suites de cifrado RC4 compatibles con el servidor remoto:

Cifras de alta resistencia (> = clave de 112 bits)

RC4-MD5 Kx = RSA Au = RSA Enc = RC4 (128) Mac = MD5
RC4-SHA Kx = RSA Au = RSA Enc = RC4 (128) Mac = SHA1

Los campos de arriba son:

{OpenSSL ciphername}
Kx = {intercambio de claves}
Au = {autenticación}
Enc = {método de cifrado simétrico}
Mac = {código de autenticación de mensaje} {bandera de exportación}

4.5.3. El nivel de cifrado de servicios de terminal server no es compatible con FIPS-140

Esta vulnerabilidad se general debido a que el servicio remoto de Servicios de Terminal Server (puerto 3389 /tcp msrdp) utiliza una configuración de cifrado que no es compatible con FIPS-140.

4.5.4. Vulnerabilidades relacionadas con el Firewall de Windows

Windows Firewall se administra a través de la Política de grupo en el servidor. Windows Firewall está deshabilitado y tiene las siguientes excepciones configuradas.

Tabla 10 excepciones configuradas en Windows Firewall

Nombre de la Conexión	Firewall	Excepciones
All Connections	Off	Ports, Programs, Services
Ethernet Off*	Off*	Ports*,Programs*,Services*
Ethernet 2	Off*	Ports*,Programs*,Services*
Ethernet 3	Off*	Ports*,Programs*,Services*
Ethernet 4	Off*	Ports*,Programs*,Services*

Fuente: Propiedad de los autores

Esta comprobación identificó que Firewall de Windows está deshabilitado en el servidor. Windows Firewall es un software de firewall que brinda protección a las computadoras al controlar qué información se transmite desde su computadora hacia y desde Internet u otras computadoras en una red. Windows Firewall está incluido en Windows Server 2008, Windows Vista, Windows XP y Windows Server 2003 Standard Edition y Enterprise Edition.

Nota

Esta comprobación se realizó de forma local sobre una copia de seguridad virtual izada del servidor por lo tanto MBSA no detecta si otro firewall (ya sea hardware o software) instalado y protege dicho servidor.

4.5.5. Vulnerabilidad en la auditoría de Windows

La comprobación determinó que la auditoría (Windows Auditing) está deshabilitada en el servidor. Microsoft Windows tiene una función de auditoría que rastrea y registra eventos específicos en su sistema, como intentos de inicio de sesión exitosos y fallidos. Al monitorear el registro de eventos de su sistema, puede ayudar a identificar posibles problemas de seguridad y actividad maliciosa.

4.5.6. Archivos Compartidos

La comprobación determinó que hay carpetas compartidas en el servidor. El informe de exploración de MBSA muestra una lista de todos los recursos compartidos que se encuentran en la computadora, incluidos los recursos

compartidos administrativos, junto con sus permisos de nivel compartido y nivel NTFS.

Debe desactivar los recursos compartidos, a menos que sea necesario, o debe protegerlos limitando el acceso a usuarios específicos.

4.5.7. Servicios potencialmente innecesarios están instalados

Esta comprobación determinó que existen servicios instalados innecesariamente, lo cual puede llegar a constituir una vulnerabilidad. Un servicio es un programa que se ejecuta en segundo plano cada vez que la computadora ejecuta el sistema operativo. No requiere que un usuario inicie sesión. Los servicios son necesarios para realizar tareas independientes del usuario, como un servicio de fax que espera a los faxes entrantes.

Los servicios en mención son los siguientes:

- MSFTPSVC (FTP)
- TlntSvr (Telnet)
- W3SVC (WWW)
- SMTPSVC (SMTP)

5. PROCEDIMIENTOS PARA MITIGAR LAS VULNERABILIDADES ENCONTRADAS

Una vez evaluadas las vulnerabilidades encontradas en el servidor de la empresa caso de estudio, los autores requirieren identificar y establecer los procedimientos que permitan el tratamiento de la vulnerabilidad y la mitigación del riesgo que esta representa para la seguridad informática y de la información de la empresa.

Fue necesario que estos se remitieran a las fuentes específicas, es decir, los proveedores de software, para este caso Microsoft, quien es el responsable de crear y distribuir las actualizaciones que permiten corregir las vulnerabilidad que sus productos puedan desarrollar al momento de la implementación; muchos de los riesgos identificados en el escaneo previo, son causados por vulnerabilidades inherentes al sistema operativo del servidor.

5.1. VULNERABILIDADES DE RIESGO CRÍTICO

5.1.1. Vulnerabilidad en HTTP.SYS - ejecución remota de código

De acuerdo al boletín de seguridad de Microsoft MS15-034 publicado el 14 de abril de 2015 y actualizado el 22 de abril de 2015, esta vulnerabilidad se mitiga instalando el parche de actualización para Windows Server 2012 R2 (3042553), esta actualización modifica la pila HTTP de Windows cambiando la forma en la cual esta gestiona las solicitudes.

La instalación del parche de actualización puede realizarse directamente mediante Windows Update, usando la ruta, Inicio →Panel de control →Seguridad → Windows Update o descargando la actualización de la página oficial de Windows en el enlace que se especifica a continuación.

Tabla 11: Actualización Vulnerabilidad en HTTP.sys

Sistema operativo	Enlace del parche de actualización
Windows Server 2012 R2 (3042553)	https://www.microsoft.com/downloads/details.aspx?familyid=3c995a85-6068-4cf0-a54d-220c2f061b95

Fuente: Boletín de seguridad de Microsoft MS15-034

5.1.2. Vulnerabilidades múltiples de Microsoft Windows SMBV1

Estas vulnerabilidades se pueden mitigar aplicando la actualización de seguridad Windows Server 2012 R2: KB4019215, la instalación del parche de actualización puede realizarse directamente mediante Windows Update, usando la ruta, Inicio →Panel de control →Seguridad → Windows Update o descargando la actualización de la página oficial de Windows.

5.1.3. Vulnerabilidad en SCHANNEL - ejecución remota de código malicioso

De acuerdo al boletín de seguridad de Microsoft MS14-066 publicado el 11 de noviembre de 2014 y actualizado el 09 de abril de 2014, esta vulnerabilidad se mitiga instalando el parche de actualización para Windows Server 2012 R2 (2992611), La actualización de seguridad corrige la vulnerabilidad mediante la corrección de cómo Schannel desinfecta los paquetes especialmente diseñados.

La instalación del parche de actualización puede realizarse directamente mediante Windows Update, usando la ruta, Inicio →Panel de control →Seguridad → Windows Update o descargando la actualización de la página oficial de Windows en el enlace que se especifica a continuación.

Tabla 12: Actualización Vulnerabilidad en Schannel

Sistema operativo	Enlace del parche de actualización
Windows Server 2012 R2 (2992611)	https://www.microsoft.com/downloads/details.aspx?familyid=bbaac95a-a997-41e1-b5ea-4687b48efe9c

Fuente: Boletín de seguridad de Microsoft MS14-066

5.1.4. Vulnerabilidad de seguridad en el servidor SMB de Microsoft Windows (Eternalchampion) (Eternalromance) (Eternalsynergy) (Wannacry) (Eternalrocks) (Petya)

De acuerdo al boletín de seguridad de Microsoft MS17-010 publicado el 14 de mayo de 2017, esta vulnerabilidad se mitiga instalando el parche de actualización de emergencia para Windows Server 2012 R2 (4012213) y (4012216). La actualización está disponible a través de Windows Update, usando la ruta, Inicio →Panel de control →Seguridad → Windows Update o descargando la actualización de la página oficial de Windows en el enlace que se especifica a continuación.

Tabla 13: Actualización Vulnerabilidad en el servidor SMB de Microsoft Windows

Sistema operativo	Enlace del parche de actualización	Actualizaciones reemplazadas
Windows Server 2012 R2 (4012213)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213	Ninguna
Windows Server 2012 R2 (4012216)	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012216	3205401

Fuente: Boletín de seguridad de Microsoft MS17-010

5.1.4.1. Método alternativo para Windows Server 2012 R2 y posteriores

Abrir el Administrador de servidores y, a continuación, hacer clic en el menú Administrar y seleccione Eliminar funciones y funciones. En la ventana Funciones, desactive la casilla de verificación SMB1.0 / CIFS File Sharing Support y, a continuación, haga clic en Aceptar para cerrar la ventana.
Reinicie el sistema.

5.1.4.2. Impacto de la solución alternativa.

El protocolo SMBv1 se deshabilitará en el sistema de destino. Para deshacer la solución. Vuelva a dibujar los pasos de solución y seleccione la casilla de verificación SMB1.0 / CIFS File Sharing Support para restaurar la característica SMB1.0 / CIFS File Sharing Support a un estado activo.

5.2. VULNERABILIDADES DE RIESGO ALTO

5.2.1. Actualizaciones de seguridad, paquetes acumulativos de actualizaciones y Service Packs

Para mitigar los riesgos relacionados a esta vulnerabilidad es necesario aplicar las actualizaciones de seguridad, instalar todos los paquetes de servicios más recientes, paquetes acumulativos de actualizaciones y actualizaciones individuales en su sistema.

La siguiente tabla identifica qué service packs, paquetes acumulativos de actualizaciones y actualizaciones de seguridad faltan en su computadora. El profesional de TI puede hacer clic en los enlaces que para ver el boletín de seguridad de Microsoft o la página de descarga, que incluye la ubicación de instalación para la actualización de seguridad.

Tabla 14 Actualizaciones de seguridad, paquetes acumulativos de actualizaciones y Service Packs

Desarrollador Herramientas, Runtimes, y Redistribuibles Seguridad Actualizaciones			
ID	**Actualización**	**Enlace**	**Causa de la actualización**
MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	https://www.microsoft.com/es-co/download/details.aspx?id=26999	Se ha identificado un problema de seguridad que provoca vulnerabilidad en las aplicaciones MFC al colocar archivos DLL que contienen código malintencionado debido a que MFC no específica la ruta de acceso completa a los archivos DLL del sistema o de localización.[55]
MS11-025	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	https://www.microsoft.com/es-co/download/details.aspx?id=26368	
Actualizaciones de seguridad e Windows			
MS14-040	Security Update for Windows Server 2012 R2 (KB2973408) without KB2919355	La actualización 2973408 es para sistemas sin la actualización 2919355 instalada. La actualización 2973408 solo está disponible a través de Windows Server Update Services (WSUS)	La vulnerabilidad podría permitir la elevación de privilegios si un atacante inicia sesión en un sistema y ejecuta una aplicación especialmente diseñada. Un atacante debe tener credenciales de inicio de sesión válida y poder iniciar sesión localmente para aprovechar esta vulnerabilidad.
2975625	Security Update for Windows Server 2012 R2 (KB2975625) without KB2919355	La actualización 2975625 solo están disponibles para clientes que manejan actualizaciones usando Windows Server Update Services (WSUS)	Esta actualización proporciona protección adicional para Local Security Authority (LSA), agrega un modo de administrador restringido para Credential Security Support Provider (CredSSP), introduce soporte para la categoría de usuario de dominio restringido por cuenta protegida y aplica políticas de autenticación más estrictas[56]

Fuente: Propiedad de los autores

[55] MICROSOFT. Microsoft.com. (2017). Actualización de seguridad de MFC para Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package from Official Microsoft Download Center. [online] Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=26999&751be11f-ede8-5a0c-058c-2ee190a24fa6=True&40ddd5bd-f9e7-49a6-3526-f86656931a02=True [Accedido 25 Nov. 2017].

[56] MICROSOFT. Docs.microsoft.com. (2017). Microsoft Security Advisory 2871997. [online] Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997 [accedido 26 Nov. 2017].

Tabla 14 (Continuación)

ID	Actualización	Enlace	Causa de la actualización
MS14-031	Security Update for Windows Server 2012 R2 (KB2961858) without KB2919355	Esta actualización solo está disponible a través de Windows Server Update	La vulnerabilidad podría permitir la denegación de servicio si un atacante envía una secuencia de paquetes especialmente diseñados al sistema de destino.[57]
MS16-100	Security Update for Windows Server 2012 R2 (KB3172729)	https://www.microsoft.com/en-us/download/details.aspx?id=53458	La vulnerabilidad podría permitir la omisión de la característica de seguridad si un atacante instala un administrador de arranque afectado y evita las características de seguridad de Windows. La actualización de seguridad corrige la vulnerabilidad al incluir en la lista negra administradores de arranque afectados.[58]
MS14-018	Windows Server 2012 R2 Update (KB2919355)	https://www.microsoft.com/es-co/download/details.aspx?id=42334	Windows Server 2012 R2 Update es u n conjunto de actualizaciones de seguridad, actualizaciones críticas y actualizaciones acumulativas. Se debe instalar Windows Server 2012 R2 Update para asegurarse de que su equipo seguirá recibiendo actualizaciones de Windows futuras, incluidas las actualizaciones de seguridad.[59]
MS14-036	Security Update for Windows Server 2012 R2 (KB2965161) without KB2919355	La actualización 2965161 solo están disponibles para clientes que manejan actualizaciones usando Windows Server Update Services (WSUS)	Esta actualización de seguridad resuelve vulnerabilidades en Windows, Microsoft Office y Microsoft Lync que podrían permitir la ejecución remota de código si un usuario abre un archivo o una página web especialmente diseñados.

Fuente: Propiedad de los autores

[57] MICROSOFT. Docs.microsoft.com. (2017). Microsoft Security Bulletin MS14-031 - Important. [online] Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-031 [Accedido 26 Nov. 2017].
[58] MICROSOFT.Docs.microsoft.com. (2017). Microsoft Security Bulletin MS16-100 - Important. [online] Disponible en: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-100 [Accedido 26 Nov. 2017].
[59] MICROSOFT. Microsoft.com. (2017). Download Windows Server 2012 R2 Update (KB2919355) from Official Microsoft Download Center. [online] Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=42334 [Accedido 26 Nov. 2017].

Tabla 14 (Continuación)

ID	Actualización	Enlace	Causa de la actualización
MS14-039	Security Update for Windows Server 2012 R2 (KB2973906) without KB2919355	https://www.microsoft.com/en-us/download/details.aspx?id=43469	La causa de esta actualización de seguridad es una vulnerabilidad en Windows que podría permitir la elevación de privilegios si un atacante usa una vulnerabilidad en un proceso de baja integridad para ejecutar el teclado en pantalla (OSK) y cargar un programa especialmente diseñado en el sistema de destino.[60]
890830	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - November 2017 (KB890830)	https://www.microsoft.com/es-co/download/malicious-software-removal-tool-details.aspx	La herramienta de eliminación de software malintencionado de Windows (MSRT) ayuda a mantener los equipos de Windows libres de malware frecuente. MSRT encuentra y elimina las amenazas e invierte los cambios que estas han llevado a cabo. MSRT se lanza mensualmente como parte de Windows Update o como una herramienta independiente cuya descarga está disponible en el enlace anteriormente relacionado.[61]

Fuente: Propiedad de los autores

[60] MICROSOFT. Support.microsoft.com. (2017). [online] Disponible en; https://support.microsoft.com/en-us/help/2973906/ms14-039-description-of-the-security-update-for-windows-on-screen-keyb [Accedido 26 Nov. 2017].
[61] MICROSOFT. Microsoft.com. (2017). Download Malicious Software Removal Tool from Official Microsoft Download Center. [online] Disponible en: https://www.microsoft.com/es-co/download/malicious-software-removal-tool-details.aspx [Accedido 26 Nov. 2017].

5.2.2. SQL Server se ejecuta en el controlador de dominio

Se recomienda que no ejecute Microsoft SQL Server en un controlador de dominio. Los controladores de dominio contienen datos confidenciales, como la información de la cuenta de usuario, y no deben utilizarse en otra función. Si ejecuta una base de datos de SQL Server en un controlador de dominio, aumenta la complejidad involucrada en la seguridad del servidor y la protección contra ataques.

La solución más viable corresponde a la ejecución de SQL Server y controladores de dominio en computadoras separadas y dedicadas.

5.2.3. Las zonas de Internet Explorer no tienen configuraciones seguras para algunos usuarios.

Para dar solución a esta vulnerabilidad se debe use la configuración recomendada en la siguiente tabla:

Tabla 15 Configuración recomendada para usuarios de Internet Explorer

Usuarios	Zona	Configuración	Selección	Recomendación
XXX\williams.avila	Internet	Descargar los controles firmados de ActiveX	Predeterminado	Deshabilitado
	Internet	Descargar de archivo	Habilitado	Deshabilitado
	Internet	Enviar datos de formulario no encriptados	Habilitado	Predeterminado

Fuente: Propiedad de los autores

Para seleccionar la configuración recomendada de zona de Internet Explorer

1. Inicie Internet Explorer.
2. En el menú Herramientas, haga clic en Opciones de Internet.
3. Haga clic en la pestaña Seguridad, haga clic en cada zona de contenido y luego en Nivel predeterminado para establecer el nivel de seguridad recomendado. Si el Nivel predeterminado no está habilitado, puede volver a habilitarlo cambiando la posición del control deslizante del nivel de seguridad.

5.3. VULNERABILIDADES DE RIESGO MEDIO

5.3.1. Vulnerabilidad de seguridad para los protocolos remotos SAM Y LSAD (3148527) (BADLOCK)

Para explotar la vulnerabilidad, un atacante podría lanzar un ataque de man-in-the-middle (MiTM), forzar una degradación del nivel de autenticación de los canales SAM y LSAD y luego suplantar a un usuario autenticado. La actualización de seguridad corrige la vulnerabilidad modificando cómo los protocolos remotos SAM y LSAD controlan los niveles de autenticación.

De acuerdo al boletín de seguridad de Microsoft MS16-047 publicado el 12 de abril de 2016, esta vulnerabilidad se mitiga instalando el parche de actualización para Windows Server 2012 R2 (3149090). La actualización está disponible a través de Windows Update, usando la ruta, Inicio →Panel de control →Seguridad → Windows Update o descargando la actualización de la página oficial de Windows en el enlace que se especifica a continuación.

Tabla 16: Actualización Vulnerabilidad en el servidor para los protocolos remotos SAM y LSAD

Sistema operativo	Enlace del parche de actualización	Actualizaciones reemplazadas
Windows Server 2012 R2 - 3149090	https://www.microsoft.com/downloads/details.aspx?familyid=c0f28b2c-883a-4acb-915f-a1d98b246a5d	3072595 en MS15-096

Fuente: Boletín de seguridad de Microsoft MS16-047

5.3.2. El certificado SSL no confiable

Evaluación de los certificados implementados para este servicio con el fin de concluir si estos son adecuados para este servicio.

Tabla 17 Salida del escaneo de certificados SSL no confiable

PUERTO	HOST	SALIDA
3389/tcp/msrdp	192.168.XXX.XXX	El siguiente certificado estaba en la parte superior de la cadena de certificados enviada por el host remoto, pero está firmada por una autoridad certificadora desconocida : | -Subject: CN = XXXXX. XXXXXXXXXXXXX.loc | -Issuer: CN = XXXXX. XXXXXXXXXXXXX.loc

Fuente: Reporte de vulnerabilidades Nessus

Tabla 17 (Continuación)

PUERTO	HOST	SALIDA
8443/tcp/www	192.168.XXX.XXX	El siguiente certificado estaba en la parte superior de la cadena de certificados enviada por el host remoto, pero está firmada por una autoridad certificadora desconocida : | -Subject: CN = F-Secure Policy Manager generó automáticamente certificado auto-firmado / CN = XXXXX. XXXXXXXXXXXXX.loc | -Issuer: CN = F-Secure Policy Manager generó automáticamente certificado auto-firmado / CN = XXXXX. XXXXXXXXXXXXX.loc

Fuente: Reporte de vulnerabilidades Nessus

5.3.3. Certificado SSL con nombre de host incorrecto

Evaluación de los certificados implementados para este servicio con el fin de concluir si estos son adecuados para este servicio.

Tabla 18 Salida del escaneo de certificados SSLL con nombre de host incorrecto

PUERTO	HOST	SALIDA
3389/tcp/msrdp	192.168.XXX.XX	Las identidades identificadas por Nessus son: 169.254.XXX.XXX 169.254.XXX.XX 169.254.XX.XXX 192.168.XXX.XXX El nombre común en el certificado es: XXXXX. XXXXXXXXXXXXX.loc
8443/tcp/www	192.168.XXX.XX	Las identidades identificadas por Nessus son: 169.254.XXX.XXX 169.254.XXX.XX 169.254.XX.XXX 192.168.XXX.XXX Los nombres comunes en el certificado son: XXXXX. XXXXXXXXXXXXX.loc F-Secure Policy Manager generó automáticamente un certificado autofirmado

Fuente: Reporte de vulnerabilidades Nessus

5.3.4. Certificado SSL auto-firmado

Evaluación de los certificados implementados para este servicio con el fin de concluir si estos son adecuados para este servicio.

Tabla 19 Salida del escaneo de certificados SSL auto-firmado

PUERTO	HOST	SALIDA
3389/tcp/msrdp	192.168.XXX.XX	El siguiente certificado estaba en la parte superior de la cadena de certificados enviada por el host remoto, pero está firmada por una autoridad certificadora desconocida : | -Subject: CN = XXXXX. XXXXXXXXXXXXX.loc
8443/tcp/www	192.168.XXX.XX	El siguiente certificado estaba en la parte superior de la cadena de certificados enviada por el host remoto, pero está firmada por una autoridad certificadora desconocida : | -Subject: CN = F-Secure Policy Manager generó automáticamente certificado auto-firmado / CN = XXXXX. XXXXXXXXXXXXX.loc

Fuente: Reporte de vulnerabilidades Nessus

5.3.5. Caché de servidores DNS - detección de información remota

Ponerse en contacto con el proveedor del software DNS para obtener una solución.

5.3.6. Vulnerabilidad en el servidor de protocolo de escritorio remoto de Microsoft Windows Man-In-The-Middle Weakness

- Forzar el uso de SSL como capa de transporte para este servicio si se admite.
- Seleccionar la opción "Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación de nivel de red" si está disponible.

5.3.7. Microsoft Windows SMB lsaquery information policy función enumeración SID sin credenciales

De acuerdo al artículo “Restringir el cheque anónimo” en Microsoft TechNet publicado el 16 de diciembre de 2009, se puede evitar búsquedas anónimas del SID de host estableciendo la configuración de Registro 'RestrictAnonymous' en un valor apropiado.

La configuración de Registro RestrictAnonymous controla el nivel de enumeración que se concede a un usuario anónimo. RestrictAnonymous se puede establecer en cualquiera de los valores siguientes:

0 -Nadie. Confíe en permisos predeterminados.
1- No permitir la enumeración de las cuentas y nombres del Administrador de cuentas de seguridad.
2 -Ningún acceso sin permisos anónimos explícitos.

No se recomienda que establezca RestrictAnonymous en 2 en controladores de dominio.

5.3.8. Firma SMB deshabilitada

Se sugiere aplicar la firma en los mensajes durante la configuración del host. Para sistemas operativos Windows, existe la opción de configurar la directiva del Servidor de red de Microsoft, habilitar como siempre. Además emplear directivas de grupo al configurar la firma SMB en caso que exista una directiva de dominio de prioridad.

5.3.9. SMB utiliza host SID para enumerar usuarios locales sin credenciales

Esta vulnerabilidad fue identificada por primera vez el 28 de abril de 1998, desde entonces Windows ha tratada de mitigar este riesgo a través de parches en los sistemas operativos, sin embargo esto no ha tenido mucho éxitos.

Sin embargo este riesgo puede llegar a mitigarse incrementando y/o fortaleciendo la seguridad perimetral de la red, ya que esta solo puede generarse siempre y cuando el atacante logre entrar a nuestra red y lazar un escaneo haciendo uso del identificador de seguridad del host (SID).

5.3.10. Suites de cifrado de tamaño de bloque SSL de 64 bits admitidas (SWEET32)

Teniendo en cuenta que tener la posibilidad de enviar ilimitadamente solicitudes en la misma conexión TLS es indispensable para que esta vulnerabilidad pueda ser explotada, la solución que resulta más obvia es la limitación de estas, así un atacante no podrá capturar información relevante trasmitida entre el cliente y el servidor en la misma conexión TLS.

Adicionalmente se deben tener en cuenta las siguientes medidas para prevenir un ataque:

- Los servidores web y las VPN deben configurarse para que prefieran cifrados de 128 bits.
- Se debe usar n navegadores web que ofrezcan 3DES como un cifrado solo de respaldo y se basen en AES, Mozilla permite esto apartar de su versión 51.
- Las bibliotecas y aplicaciones TLS deben limitar la duración de las sesiones TLS con un cifrado de 64 bits. Esto podría hacerse con la renegociación de TLS, o en algunos casos cerrando la conexión e iniciando una nueva (es decir, limitando HTTP / 1.1 Keep-Alive, SPDY y HTTP / 2 con 3DES ciphersuites).
- Cambiar el cifrado predeterminado a AES, usando cifrados de 128 bits para la configuración del cliente y del servidor.

5.3.11. Certificado SSL firmado utilizando algoritmo de HASH débil

La solución es la reedición de los certificados de seguro haciendo uso de un algoritmo criptográfico más seguro.

La anterior solución es la única posible ya que esta vulnerabilidad no obedece a una falla en el sistema operativo tal como lo expreso Microsoft en su aviso de seguridad 961509 publicado el 30 de diciembre de 2008, esta vulnerabilidad es conocida por las entidades certificadoras quienes están trabajando en la implementación de algoritmos más seguros y seguramente bridaran todo el apoyo requerido para la creación de los certificados con algoritmos más eficientes.

5.3.12. Soporte de cifrado SSL de mediana intensidad

La solución más conveniente es evitar el uso de cifrados de intensidad media y reemplazarlos por cifrados más seguros que permitan el uso una cantidad de bits superiores a 128.

5.3.13. Servicios de terminal server no utiliza autenticación de nivel de red (NLA)

La solución es sencilla y consiste en habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto.

Las ventajas de usar la autenticación de nivel de red (NLA) son:

- Consume una cantidad menor de recursos de la computadora remota inicialmente. La máquina remota utiliza una cantidad limitada de recursos antes de autenticar al usuario.
- proporciona mayor seguridad y reduce el riesgo de ataques de denegación de servicio.

Para configurar la autenticación de nivel de red (NLA) es necesario seguir los siguientes pasos establecidos por Microsoft en el artículo de su foro technet "Configurar la autenticación de nivel de red para conexiones de servicios de escritorio remoto":

1. En el servidor Host de sesión de RD, abra Configuración de host de sesión de escritorio remoto. Para abrir Configuración de host de sesión de escritorio remoto, haga clic en Inicio, seleccione Herramientas administrativas, seleccione Servicios de escritorio remoto y luego haga clic en Configuración de host de sesión de escritorio remoto.
2. En Conexiones, haga clic derecho en el nombre de la conexión y luego haga clic en Propiedades.
3. En la pestaña General, seleccione Permitir conexiones solo desde equipos que ejecutan la casilla de verificación Escritorio remoto con autenticación de nivel de red.
4. Si la casilla Permitir conexiones solo de equipos que ejecutan el Escritorio remoto con Autenticación de nivel de red está activada y no está habilitada, se ha habilitado la autenticación Requerir autenticación de usuario para conexiones remotas mediante la configuración de Directiva de grupo de autenticación de nivel de red y se ha aplicado al host de sesión de RD servidor.
5. Haga clic en OK.[62]

5.3.14. El nivel de cifrado de servicios de terminal server es medio

La solución es muy sencilla, consiste en cambiar el nivel de cifrado RDP a uno Alto compatible con FIPS.

[62] Configurar la autenticación de nivel de red para conexiones de servicios de escritorio remoto, basado en https://technet.microsoft.com/en-us/library/cc732713.aspx

Para cambiar el nivel de cifrado RDP a uno Alto compatible con FIPS del servidor para una conexión, es necesario seguir los siguientes pasos establecidos por Microsoft en el artículo de su foro technet “Configuración de la autenticación y los niveles de cifrado del servidor”:

1. En el servidor de host de sesión de Escritorio remoto, abra Configuración de host de sesión de Escritorio remoto. Para abrir Configuración de host de sesión de Escritorio remoto, haga clic en Inicio, seleccione Herramientas administrativas, seleccione Servicios de Escritorio remoto y, a continuación, haga clic en Configuración de host de sesión de Escritorio remoto.
2. En Conexiones, haga clic con el botón secundario en el nombre de la conexión y, a continuación, haga clic en Propiedades.
3. En el cuadro de diálogo Propiedades para la conexión, en la ficha General, seleccione la autenticación del servidor y la configuración de cifrado adecuada para el entorno, según sus requisitos de seguridad y el nivel de seguridad que los equipos cliente pueden admitir.
4. Si elige SSL (TLS 1.0), seleccione un certificado que esté instalado en el servidor de Host de sesión de Escritorio remoto o haga clic en Predeterminado para generar un certificado autofirmado. Si va a usar un certificado autofirmado, su nombre se mostrará como Generado automáticamente.
5. Haga clic en Aceptar.[63]

5.3.15. Vulnerabilidad de denegación de servicios TCP/IPv4

De acuerdo al Boletín de seguridad MS13-018 [64] de Microsoft publicado el 12 de febrero de 2013 y actualizado el 12 de febrero de 2013, esta vulnerabilidad se debe mitigar instalando una actualización de seguridad, si esta se omite y no se instala la vulnerabilidad podría permitir la denegación de servicio si un atacante no autenticado envía un paquete de terminación de conexión especialmente diseñado al servidor.

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Windows Server 2008, Windows Server 2008 R2 y Windows Server 2012; está clasificado como Moderado para todas las ediciones compatibles de Windows Vista, Windows 7, Windows 8 y Windows RT. La actualización de seguridad mitiga la vulnerabilidad al corregir cómo la pila TCP / IP de Windows maneja las secuencias de terminación de la conexión.

[63] Configuración de la autenticación y los niveles de cifrado del servidor, basado en https://technet.microsoft.com/es-es/library/cc770833(v=ws.11).aspx

[64] MICROSOFT. Docs.microsoft.com. (2017). Microsoft Security Bulletin MS13-018 - Important. [online] Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2013/ms13-018 [Accedido 17 Nov. 2017].

Microsoft recomienda que los clientes apliquen la actualización lo antes posible, lo cual se puede realizar mediante el software de administración de actualizaciones o buscando las actualizaciones utilizando el servicio Microsoft Update.

Tabla 20 Actualización para mitigar la vulnerabilidad de denegación de servicios TCP/IPv4

Sistema operativo	Enlace del parche de actualización	Impacto máximo de seguridad	Clasificación de gravedad agregada	Actualizaciones reemplazadas
Windows Server 2012 (KB2790655)	http://www.microsoft.com/downloads/details.aspx?familyid=f74a104d-4749-4dd5-b144-2e4ce9c284a2	Negación de servicio	Importante	Ninguna

Fuente: Boletín de seguridad de Microsoft MS13-018

5.3.16. Vulnerabilidad en los informes de enumeración de servicios de MSRPC

La solución para la mitigación de esta vulnerabilidad consiste en filtrar el tráfico entrante a los puertos usados por este servicio. (Los puertos usados por el servicio MSRPC pueden detallasen en los resultados del escaneo con la herramienta NMAP. Pág. 60)

El filtrado de estos puertos se puede realizar utilizando firewalls basados en host o filtros IPSec. No se recomienda deshabilitar el servicio RPC, se puede deshabilitar DCOM para evitar vulnerabilidades específicas que involucran la interfaz RPC/DCOM. Si bien desactivar DCOM no es tan debilitante como deshabilitar RPC, probablemente cause problemas con sus aplicaciones de Windows, así que se debe tener mucho cuidado si elige esta opción.

Aunque Microsoft insta a todos los clientes a aplicar parches a la primera oportunidad posible, existe una serie de soluciones que se pueden aplicar para ayudar a evitar que el vector utilizado explote esta vulnerabilidad. No hay garantía de que las soluciones bloquearán todos los posibles vectores de ataque.

a) Bloquee los puertos UDP 135, 137, 138, 445 y los puertos TCP 135, 139, 445, 593 en el cortafuegos y deshabilite los Servicios de Internet COM (CIS) y RPC sobre HTTP, que escuchan en los puertos 80 y 443, en los sistemas afectados.

Estos puertos se utilizan para iniciar una conexión RPC con una computadora remota. Bloquearlos en el firewall ayudará a evitar que los sistemas detrás de ese firewall sean atacados por los intentos de explotar estas vulnerabilidades. También debe asegurar y bloquear cualquier otro puerto RPC específicamente configurado en la máquina remota. Si está habilitado, CIS y RPC sobre HTTP permiten que las llamadas DCOM operen a través de los puertos TCP 80.

b) Bloquear los puertos afectados utilizando un filtro IPSEC y deshabilite los Servicios de Internet COM (CIS) y RPC sobre HTTP, que escuchan en los puertos 80 y 443, en las máquinas afectadas.

Se puede proteger las comunicaciones de red en equipos con Windows si se usa Internet Protocol Security (IPSec).

5.3.17. Puertos UDP abiertos sin administrar

Nmap identifico 29 puertos UDP abiertos, de los cuales tan solo 3 tienen un servicio en ejecución, los 26 puertos restantes no tienen un servicio activo, por tanto constituyen un riesgo para la seguridad de la información, para mitigar esta vulnerabilidad se deber seguir el procedimiento indicado por Microsoft para cerrarlos.[65]

1) Abrir la Consola de Windows SBS.
2) En la barra de navegación, haga clic en Red y, a continuación, en Conectividad.
3) Haga clic con el botón secundario en Firewall del servidor y, a continuación, haga clic en Ver propiedades del firewall.
4) Haga clic en la ficha Opciones avanzadas y, a continuación, haga clic en Administrar reglas.
5) Haga clic en Dejar pasar a un programa a través de Firewall de Windows.
6) En la ficha Excepciones, desplácese en el cuadro de texto Programa o puerto hasta encontrar el nombre del puerto que desea cerrar.
7) Si desea deshabilitar el puerto de forma temporal, desactive la casilla de verificación y haga clic en Aceptar.

[65] MICROSOFT, Technet.microsoft.com. (2017). Cerrar puertos en el firewall del servidor. [online] Disponible en: https://technet.microsoft.com/es-es/library/dd353101(v=WS.10).aspx [Accedido 18 Nov. 2017].

8) Si no planea usar el programa que requiere ese puerto, haga clic en Eliminar para eliminar de forma permanente el nombre del programa y el número de puerto, luego haga clic en Sí y, a continuación, en Aceptar.

5.3.18. Cuentas de usuario con contraseñas sin vencimiento.

Una cuenta local que tenga una configuración de Contraseña que nunca caduca anulará la configuración de Máxima edad de contraseñas en la Política de grupo, lo que permite que el usuario conserve la misma contraseña para siempre.

Cuando los administradores o los operadores de la mesa de ayuda asignan nuevas contraseñas a los usuarios, es una buena práctica establecer que el usuario debe cambiar la contraseña en la próxima opción de inicio de sesión para asegurarse de que el usuario establezca una nueva contraseña.

Todas las cuentas locales identificadas en el informe de seguridad que tengan contraseñas que no caducan deben revisarse para determinar por qué se establece la opción y si debe eliminarse.

Para borrar la configuración de Contraseña nunca caduca en las plataformas de Microsoft Windows siga los siguientes pasos:

1) Abra el Panel de control.
2) Haga doble clic en Herramientas administrativas y luego haga doble clic en Administración de equipos.
3) Haga doble clic en la carpeta Usuarios y grupos locales, y luego haga clic en la carpeta Usuarios.
4) En el panel derecho, haga doble clic en la cuenta que desea cambiar.
5) En el cuadro de diálogo Propiedades, desactive la casilla de verificación La contraseña nunca caduca.

Precaución

Los administradores no deben eliminar la configuración de Contraseña nunca caduca para las siguientes cuentas, ya que hacerlo puede interrumpir la funcionalidad de la aplicación y el servidor:

- IUSR_ <nombre de computadora>
- IWAM_ <nombre de computadora>
- TSInternetUser

5.3.19. Se encontraron más de 2 administradores en el servidor.

Las cuentas de usuario que pertenecen a los grupos Administradores locales o Administradores de dominio tienen autoridad para hacer casi cualquier cosa en los sistemas y redes a los que tienen permiso de acceso. Si dicha cuenta se toma de forma maliciosa, se podría causar un daño catastrófico al sistema o a la red.

Es importante revisar la lista de miembros en los grupos Administradores locales y Administradores de dominio para garantizar que todos los usuarios con autoridad administrativa estén justificados. Se recomienda mantener el número de administradores al mínimo, porque los administradores esencialmente tienen control total sobre la computadora.

5.4. VULNERABILIDADES DE RIESGO BAJO

5.4.1. Detección de servidor DHCP

Dar solución a esta vulnerabilidad relacionada con la detección de servicios es relativamente fácil ya que esta se puede mitigar aplicando filtros para mantener la información obtenido fuera de la red y como complemento de esto es necesario eliminar cualquier otra opción que no esté en uso.

5.4.2. SSL RC4 CIPHER SUITES soportado (BAR MITZVAH)

Para dar solución a esta vulnerabilidad es necesario evaluar la posibilidad de usar TLS 1.2 con suites AES-GCM sujetas a compatibilidad con el navegador y el servidor web o en su defecto reconfigurar las aplicaciones que puedan llegar a verse afectadas para evitar en lo posible el uso de cifrados RC4.

5.4.3. El nivel de cifrado de servicios de terminal server no es compatible con FIPS-140

La solución es muy sencilla, consiste en cambiar el nivel de cifrado RDP a uno Alto compatible con FIPS.

Para cambiar el nivel de cifrado RDP a uno Alto compatible con FIPS del servidor para una conexión, es necesario seguir los siguientes pasos establecidos por Microsoft en el artículo de su foro technet “Configuración de la autenticación y los niveles de cifrado del servidor”:

1. En el servidor de host de sesión de Escritorio remoto, abra Configuración de host de sesión de Escritorio remoto. Para abrir Configuración de host de sesión de Escritorio remoto, haga clic en Inicio, seleccione Herramientas administrativas, seleccione Servicios de Escritorio remoto y, a continuación, haga clic en Configuración de host de sesión de Escritorio remoto.
2. En Conexiones, haga clic con el botón secundario en el nombre de la conexión y, a continuación, haga clic en Propiedades.
3. En el cuadro de diálogo Propiedades para la conexión, en la ficha General, seleccione la autenticación del servidor y la configuración de cifrado adecuada para el entorno, según sus requisitos de seguridad y el nivel de seguridad que los equipos cliente pueden admitir.
4. Si elige SSL (TLS 1.0), seleccione un certificado que esté instalado en el servidor de Host de sesión de Escritorio remoto o haga clic en Predeterminado para generar un certificado autofirmado. Si va a usar un certificado autofirmado, su nombre se mostrará como Generado automáticamente.
5. Haga clic en Aceptar.[66]

5.4.4. Vulnerabilidades relacionadas con el Firewall de Windows

Windows Firewall es un software de firewall que brinda protección a las computadoras al controlar qué información se transmite desde su computadora hacia y desde Internet u otras computadoras en una red. Windows Firewall está incluido en Windows Server 2008, Windows Vista, Windows XP y Windows Server 2003 Standard Edition y Enterprise Edition.

El servidor escaneado no tiene Firewall de Windows habilitado en todas las conexiones de red.

Para dar solución a esta vulnerabilidad se debe habilitar el Firewall de Windows en cada conexión de red en su computadora, siguiendo las siguientes instrucciones:

Debe iniciar sesión como administrador o miembro del grupo Administradores para completar este procedimiento. Si el servidor está conectado a una red, la configuración de la política de red también puede evitar que complete este procedimiento.

1) Abra Inicio, y luego haga clic en el Panel de control.
2) Haga clic en el ícono de Firewall de Windows.

[66] Configuración de la autenticación y los niveles de cifrado del servidor, basado en https://technet.microsoft.com/es-es/library/cc770833(v=ws.11).aspx

3) Seleccione Activar o desactivar Firewall de Windows, luego seleccione Activado (recomendado).

Nota

Esta comprobación se realizó de forma local sobre una copia de seguridad virtual izada del servidor por lo tanto MBSA no detecta si otro firewall (ya sea hardware o software) instalado y protege dicho servidor.

5.4.5. Vulnerabilidad en la auditoría de Windows

La auditoría es un paso vital para detectar intrusiones del sistema o actividad maliciosa en sus sistemas y redes. El Visor de sucesos de Windows no registra entradas de eventos en el registro de seguridad a menos que active la auditoría en el sistema.

Para dar solución a esta vulnerabilidad debe habilitar la auditoría en el servidor. Después de habilitar la auditoría, puede elegir qué eventos supervisar, como intentos de inicio de sesión exitosos o fallidos. Además, ciertos archivos y directorios pueden auditarse en sistemas de archivos NTFS para modificaciones o eliminaciones. Vea los enlaces en la sección Recursos adicionales a continuación para obtener más información sobre la configuración de las políticas de auditoría.

Para habilitar la auditoría en el servidor siga los siguientes pasos:

1) Abra el Panel de control.
2) En el Panel de control, haga doble clic en Herramientas administrativas y luego haga clic en Política de seguridad local.
3) En Configuración de seguridad local, haga doble clic en Políticas locales, haga doble clic en Política de auditoría y luego haga clic en los eventos que desea auditar. recomendamos que audite los siguientes eventos:

- Eventos de inicio de sesión de cuenta de auditoría (éxito, error)
- Gestión de cuentas de auditoría (éxito, fracaso)
- Auditar el acceso al servicio de directorio (Error)
- Eventos de inicio de sesión de auditoría (éxito, error)
- Acceso a objetos de auditoría (falla)
- Cambio de política de auditoría (éxito, falla)
- Eventos del sistema de auditoría (éxito, falla)

Para ver los registros de eventos, haga clic en Inicio, señale Programas, señale Herramientas administrativas y luego haga clic en Visor de eventos.

5.4.6. Archivos Compartidos

Los sistemas operativos Microsoft Windows permiten a los usuarios compartir archivos con otros usuarios. Sin embargo, si un recurso compartido no está protegido adecuadamente, los usuarios no autorizados podrían tener acceso a la información del recurso compartido.

Debe desactivar los recursos compartidos, a menos que sea necesario, o debe protegerlos limitando el acceso a usuarios específicos. Los permisos compartidos deben revisarse para garantizar que el acceso se limite solo a usuarios autorizados y no se comparta con todos.

Para deshabilitar un recurso compartido el servidor siga las siguientes pasos:

1) Abra el Panel de control.
2) Haga doble clic en Herramientas administrativas y luego haga doble clic en Administración de equipos.
3) Haga clic con el botón derecho en el recurso compartido para desactivar el recurso compartido o cambiar los permisos de uso compartido.

5.4.7. Servicios potencialmente innecesarios están instalados

El administrador del servidor debe determinar si los servicios MSFTPSVC (FTP), TlntSvr (Telnet), W3SVC (WWW), SMTPSVC (SMTP) son necesarios. Si es innecesario, deberían estar deshabilitados. Por ejemplo, si se encuentra que el servicio Telnet está instalado y habilitado, pero los usuarios no están obligados a conectarse remotamente a través de Telnet a esa computadora específica, este servicio debe estar deshabilitado.

Use los Servicios en el Panel de control para deshabilitar los servicios en ejecución que no deberían ejecutarse en el servidor. Los servicios que están habilitados pero no son obligatorios pueden representar un riesgo para la seguridad de la computadora.

Para deshabilitar servicios en el servidor siga las siguientes instrucciones:

1) Abra el Panel de control.
2) Haga doble clic en Herramientas administrativas y luego haga clic en Servicios.
3) Haga doble clic en el servicio que desea deshabilitar.
4) Haga clic en Detener para detener el servicio.
5) En Tipo de inicio, haga clic en Deshabilitado.

Importante:

Si está ejecutando Small Business Server (SBS), hay servicios enumerados en MBSA que son esenciales para la funcionalidad de su servidor. Estos son los servicios de Simple Mail Transport Protocol (SMTP) y World Wide Web Publishing. No desactive estos servicios en computadoras con SBS.

RECOMENDACIONES

No ejecutar SQL Server en un controlador de dominio. Los controladores de dominio contienen datos confidenciales y no deben utilizarse en otra función. Si ejecuta una base de datos de SQL Server en un controlador de dominio, aumenta la complejidad involucrada en la seguridad del servidor y la protección contra ataques.

Emplear una depuración de puertos en todos los servidores de la empresa caso de estudio, permitiendo que solo sea posible el tráfico en los puertos necesarios y que son necesarios para que se da la continuidad del negocio y hacer la documentación de este proceso.

Verificar que todos los sistemas de autenticación se encuentren actualizados y bien definidos en cuanto a robustez de las credenciales de acceso, tiempo de caducidad y roles de cada usuario. Además, verificar que los servicios considerados críticos cuenten con un sistema de autenticación.

Inspeccionar la configuración del firewall en todas las estaciones de trabajo, bloqueando todos los puertos que no se usen.

Revisar las Políticas de Seguridad actuales de la empresa, modificando o agregando las necesarias, que permitan atender los problemas de seguridad evidenciados en los resultados del escaneo de vulnerabilidades.

Hacer consiente a todo el personal de la empresa sobre la importancia de conocer y aplicar las Políticas de Seguridad implementadas en la empresa.

Capacitar a los empleados de acuerdo a su rol sobre cada una de las políticas de seguridad definidas.

Para futuros escaneos de vulnerabilidades, este documento debe ser una consulta relevante a ser tomada en cuenta por los involucrados en dicho proceso y así evitar ser redundantes en procesos y atender las necesidades de seguridad que en el momento requiera la empresa caso de estudio.

Para obtener e instalar las actualizaciones más recientes y para usar efectivamente los resultados de MBSA, observe estas pautas:

a) Visite el sitio web Microsoft Update para instalar las actualizaciones, a menos que se necesite más control sobre las actualizaciones que desea instalar o descargar. La ubicación del paquete de descarga está disponible en la columna Descargar del informe. Los paquetes generalmente están en formato

EXE, MSI o CAB, y se pueden guardar o abrir después de hacer clic en el ícono Descargar.

b) Regístrese en el Servicio de notificación de seguridad de Microsoft para asegurarse de recibir una notificación cuando haya nuevos boletines de seguridad disponibles.
c) Al actualizar su computadora, recuerde que los cambios en la configuración pueden requerir el uso adicional de Microsoft Update o MBSA para verificar que la nueva configuración cumpla con los requisitos. Esto es particularmente cierto cuando se instalan aplicaciones o cuando se agregan nuevos componentes opcionales, como Internet Information Services (IIS), que pueden instalar programas que no se han actualizado con las últimas correcciones.

CONCLUSIONES

Un puerto en un equipo informático se asemeja a las puertas o ventanas de una casa, donde se puede ingresar y salir cuantas veces se desee por la puerta principal, pero aquí existe el riesgo de que un ladrón ingrese por la ventana, incluso por la misma puerta principal pasando desapercibido; es por eso que en el caso de los puertos, si no se tienen las medidas de seguridad requeridas, serán explotados trayendo como resultado que se observe la computadora, se presente el robo de datos confidenciales, espiar la actividad que se realiza en los mismos, entre otros.

Un puerto que se encuentra abierto, en principio no representa un alto peligro, se presenta el riesgo siempre y cuando el software que hace uso del mismo contiene código malicioso. Los puertos no son ejecutados directamente por el sistema operativo, estos se abren cuando un programa necesita hacer uso del mismo.

En la cotidianidad hay puertos como el 21 que se emplea para la descarga de archivos que están alojados en servidores FTP; puertos como el 25 comúnmente usado en el correo electrónico; el famoso puerto 80 generalmente usada en todas las comunicaciones que son requeridas para que funcione una página web y el puerto 110 también empleado en correo electrónico. Como se observa estos puertos no representan peligro alguno y son necesarios en las tareas cotidianas y en el uso de los servicios del internet.

En el sistema operativo Windows, se encuentra una aplicación llamada NETSTAT, la cual se usa por medio de la consolada de comandos, esta permita saber con exactitud los puertos abiertos e inclusive cuales de esos trasmiten y envían datos hacia el exterior.

Las actualizaciones de seguridad en un sistema operativo o aplicación agregan nuevas funciones, fortalecen las que ya posee y dan solución a las vulnerabilidades y fallos de seguridad detectados. Es por eso en el área de la seguridad informática, tener al día todas las actualizaciones en cada estación de trabajo, además ejecutar e instalar los parches de seguridad sugeridos por los fabricantes de software, esto ayudara en gran medida a prevenir las infecciones por virus, malware, adware, entre otros, de esta manera evitar que en los sistemas ingresen los hackers.

Es importante tener actualizado el sistema de antivirus en las estaciones de trabajo, no solo basta con tener las versiones más recientes, si este no está actualizado y así no es capaz de detectar las más recientes amenazas que deambulan por la red de redes.

Los delincuentes informáticos han empleado en los últimos años la instalación de parches, donde han logrado infectar un equipo informático. Por tal motivo hay que ser muy precavidos en los sitios web que se visitan donde se ofrecen la instalación de actualizaciones falsas. Por tal motivo solo se deben instalar las actualizaciones desde sitios web oficiales.

Al identificar las vulnerabilidades se propusieron las respectivas recomendaciones y/o soluciones que harán posible mitigar las vulnerabilidades encontradas.

Establecer una serie de políticas de seguridad y manual de buenas prácticas dentro de una organización, ayudara a minimizar el riesgo de vulnerabilidad en los sistemas que en ella residen.

Un sistema operativo siempre se encuentra expuesto a infinidad de ataques, por este motivo su seguridad es primordial, pero gracias a la infinidad de herramientas, aplicaciones, distribuciones, ente otras, se ha mejorado cada vez más en cuanto a la seguridad de los SO, los desarrolladores de malware están a la orden del día, pero también están las aplicaciones encargadas de eliminar las vulnerabilidades, es una guerra que se libra en un campo virtual, donde los ataques son constantes y las defensas de los SO deben estar siempre disponibles y con el arsenal de más alta calidad disponible, todo esto con el fin de garantizar la información contenida en equipos.

Gracias a la realización de este proyecto, la empresa caso de estudio ha decido crear un grupo de profesionales con la capacitación idónea, integrado por funcionarios de múltiples gerencias departamentales, para replicar lo expuesto, implementar los procedimientos sugeridos para la mitigación de las vulnerabilidades y monitorear, verificar y mantener la seguridad informática de la información y los activos de TI en el nivel de riesgo óptimo para la organización.

BIBLIOGRÁFIA

AGUILERA LÓPEZ, P. Seguridad Informática (1st ed.). Editex. (2010).

AGUILERA, Purificación. Seguridad informática. 1 ed. España: Editex. 2010, 240 p

BENAVIDES ARIAS, Andrés Fernando y VELÁSQUEZ MAYORGA, John Freddy. Prueba de intrusión al sistema operativo Windows Server 2003 de una empresa del sector financiero. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Medellín. 2015.

BENCHIMOL, D. Hacking desde cero (1st ed.). Buenos Aires: Fox Andina. (2011).

CANDELA Solá, S. Fundamentos de sistemas operativos (1st ed.). Madrid: Paraninfo. (2011).

CANDELA, Santiago *et al*. Fundamentos de Sistemas Operativos. 1 ed. España: S.A Ediciones Parainfo. 2007, 712 p.

CHICANO TEJADA, Ester. Auditoria de seguridad informática. 1 ed. España: IC Editorial. 2014.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266 de 2008 Nivel Nacional. Bogotá .Diario Oficial 47.2. 19 de diciembre 31 de 2008.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Diario Oficial 47.223. Bogotá. (Enero 5 de 2009)

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 23 de 1982 Nivel Nacional. Bogotá. Diario Oficial. 28 de enero de 1982

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527. Diario Oficial 43.673 del 21 de agosto de 1999. Bogotá. (Agosto 18 de 1999)

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 DE 2000. Diario Oficial 44097. Bogotá. Julio 24 de 2000

COLOMBIA, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL – CONPES. Documento CONPES 3854. Bogotá. (Julio 14 de 2011)

COLOMBIA, CORTE CONSTITUCIONAL, Sentencia C-662. Diario Oficial No. 48.308 Bogotá. (Junio 6 de 2000)

COLOMBIA. . CONSTITUCION POLITICA DE COLOMBIA. Bogotá. D.C. 1991

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1360 (23 de junio) Bogotá. D.C. 1995

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1747 (11 de Septiembre). DIARIO OFICIAL No. 44.160, Bogotá, jueves 14 de septiembre de 2000. Bogotá. D.C. 2000

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 460 (16 de marzo) Bogotá. D.C. 1995

COSTAS SANTOS, J. Mantenimiento de la seguridad en sistemas informáticos (1st ed.). (2014).

DESONGLES CORRALES, J. Ayudante técnico de informática de la Junta de Andalucía (1st ed.). Sevilla: Editorial MAD. (2005).

DIAZ ORUETA, Gabriel; ALZÓRRIZ ARMENDÁRIZ, Ignacio; SANCRISTÓBAL RUIZ, Elio; CASTRO GIL, Manuel A. Procesos y herramientas para la seguridad de redes. 1 ed. España: Universidad Nacional de Educación a Distancia. 2014.

ECHEVERRIA, G. Procedimientos y Medidas de Seguridad Informática (1st ed.). Paperback. (2008).

EE. UU, INTERNET ENGINEERING TASK FORCE (IETF), RFC 2196 – Site Security Handbook. Fremont, California. (Diciembre 3 de 2014)

FLORES ROSA, Marco A. Windows Server R2. 1 ed. Perú: S.A Editorial Macro. 2014, p 555.

GIMÉNEZ ALBACETE, José F. Seguridad en equipos informáticos. 1 ed. España: IC Editorial. 2014, 548 p.

GÓMEZ Vieites, A. Seguridad en equipos informáticos (1st ed.). (2014).

GONZÁLEZ POMBO, Alexandra Milena y GÓMEZ BARBOZA, Orlando. Identificar las vulnerabilidades en el manejo de la información y formular las políticas de Gobierno de Tecnología para el manejo seguro de la aplicación SIREP del CCAV Cartagena. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Cartagena. 2015.

GUERRERO ERAZO, Henry Aldemar et al. 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. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Pasto. 2015.

GUERRERO ERAZO, Henry Aldemar et al. 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. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Pasto. 2015.

HANDZ, Valentín. Windows 7 y sus Novedades. 1 ed. Handsofthelp. p 30.

JARA, Héctor; PACHECO, Federico G. Ethical Hacking 2. 1 ed. Creative Andina Corp. 2009, 310 p.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27001. Ginebra, Suiza. (Octubre de 2013)

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 17799. Ginebra, Suiza. (Junio de 2005)

RAMA JUDICIAL DEL PODER PÚBLICO CONSEJO SUPERIOR DE LA JUDICATURA. Sala Administrativa. Bogotá. (Marzo de 2006)

SILES RAUL, Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Primera Edición, (2002.)

SOMMERVILLE, I., & ALFONSO Galipienso, M. Ingeniería del software (1st ed.). Madrid: Pearson Educación. (2005).

SOMMERVILLE, Ian. Ingeniería del Software. 1 ed. España: Pearson Education. 2005, 712 p.
STAFF, U. Hacking desde cero (1st ed.). Creative Andina Corp. (2011).

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD. Resolución 004256. (3, marzo, 2015). Por la cual se define las políticas del Marco de Referencias del SGSI. Bogotá. 2015

VIVER RAMIREZ, Aydee Mercedes. Identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de Pentesting. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Cali. 2016.

WEBGRAFIA

ALCALDIA BOGOTA. Consulta de la Norma. (En línea). Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

BLOG SOBRE INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN. (26 de octubre de 2012). Disponible en internet: http://marcosjgutierrez.blogspot.com.co/2012/10/diferencias-entre-ethical-hacking.html

C. TIEMPO, "La ciberdelincuencia no segmenta: todos somos vulnerables", Portafolio.co. (En línea). Disponible en: http://www.portafolio.co/opinion/otros-columnistas-1/ciberdelincuencia-colombia-perdidas-anuales-155222.

CATOIRA, F. Penetration Test, ¿en qué consiste? WeLiveSecurity. (En línea). Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

CORTE CONSTITUCIONAL. Sentencia C-662/00. (En línea). Disponible en: http://www.corteconstitucional.gov.co/relatoria/2000/C-662-00.html

HERNÁNDES PÉREZ, Flor A, *et al*. Glosario de términos informáticos [en línea]. El Cid Editor Editorial, 2006. ISBN E-BOOK: 978-141-35-6491-4. 102 p. Disponible en internet: http://bibliotecavirtual.unad.edu.co:2460/lib/unadsp/reader.action?docID=3167493

INSTITUTO DISTRITAL DE TURISMO. (En línea). Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

KALI LINUX. Política de Código Abierto en Kali Linux. (En línea). Disponible en: http://es.docs.kali.org/kali-policy-es/politica-de-codigo-abierto-en-kali-linux

LOPEZ, David. Evolución de la Seguridad Informática [En línea]. Grupo Control Seguridad. Disponible en Internet: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica

MICROSOFT. Acuerdos de Licencia Microsoft. (En línea). Disponible en: https://www.microsoft.com/Argentina/PUBLIC/KIT_BASE/LICENCIAMIENTO/LICSEMGT/mslicns/EULAs.htm

MICROSOFT. Docs.microsoft.com. (2017). Microsoft Security Advisory 2871997. [Online] Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997
MICROSOFT. Docs.microsoft.com. (2017). Microsoft Security Bulletin MS14-031 - Important. [Online] Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-031

MICROSOFT. Microsoft.com. (2017). Actualización de seguridad de MFC para Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package from Official Microsoft Download Center. [Online] Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=26999&751be11f-ede8-5a0c-058c-2ee190a24fa6=True&40ddd5bd-f9e7-49a6-3526-f86656931a02=True

MICROSOFT. Microsoft.com. (2017). Download Malicious Software Removal Tool from Official Microsoft Download Center. [Online] Disponible en: https://www.microsoft.com/es-co/download/malicious-software-removal-tool-details.aspx

MICROSOFT. Microsoft.com. (2017). Download Malicious Software Removal Tool from Official Microsoft Download Center. [Online] Disponible en: https://www.microsoft.com/es-co/download/malicious-software-removal-tool-details.aspx

MICROSOFT. Microsoft.com. (2017). Download Windows Server 2012 R2 Update (KB2919355) from Official Microsoft Download Center. [Online] Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=42334

MICROSOFT. Support.microsoft.com. (2017). [Online] Disponible en; https://support.microsoft.com/en-us/help/2973906/ms14-039-description-of-the-security-update-for-windows-on-screen-keyb

MICROSOFT. Support.microsoft.com. (2017). [Online] Disponible en; https://support.microsoft.com/en-us/help/2973906/ms14-039-description-of-the-security-update-for-windows-on-screen-keyb

MICROSOFT. Windows Server 2012 – Nuevo Licenciamiento. (2017). IT PRO Colombia. (En línea). , disponible en: https://blogs.technet.microsoft.com/itprocol/2012/07/11/windows-server-2012-nuevo-licenciamiento/

MICROSOFT.Docs.microsoft.com. (2017). Microsoft Security Bulletin MS16-100 - Important. [Online] Disponible en: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-100

MIFSUD, E. (2017). MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático | Observatorio Tecnológico. [En línea] Recursostic.educacion.es. Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2017). [En línea] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINITIC. (2017). Sistemas de Gestión de la Seguridad de la Información (SGSI). (En línea). Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL (2017). [Online] Disponible en: http://www.wipo.int/treaties/es/convention/summary_wipo_convention.html

RAMÍREZ MONTAÑEZ, J. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona Norte de Santander. Colombia. (2015). Disponible en: http://hdl.handle.net/10596/3415

THE INTERNET ENGINEERING TASK FORCE. (En línea). Disponible en: https://www.ietf.org/rfc/rfc2196.txt

ANEXOS

Anexo A Resumen General Vulnerabilidades Halladas con Nessus

Nessus Report
Nessus Scan Report
Mon, 20 Nov 2017 07:43:28 GMT-0500

Detalles del escaneo

IP:	192.168.XXX.XXX
DNS:	xxxxxxxxxxxxxxx
MAC:	xxxxxxxxxxxxxxx
OS:	Microsoft Windows Server 2012 R2 Standard
Inicio:	7:43 AM
Fin:	7:48 AM
Duración:	5 minutes

Vulnerabilidades

192.168.XXX.XXX

Summary

Critical	High	Medium	Low	Info	Total
4	0	14	3	61	82

Details

Severity	Plugin Id	Name
Critical (10.0)	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
Critical (10.0)	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Critical (10.0)	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	56210	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials
Medium (5.0)	56211	SMB Use Host SID to Enumerate Local Users Without Credentials
Medium (5.0)	57608	SMB Signing Disabled
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (3.3)	10663	DHCP Server Detection
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10394	Microsoft Windows SMB Log In Possible
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULLSession Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10897	Microsoft Windows - Users Information : Disabled Accounts
Info	10899	Microsoft Windows - Users Information : User Has Never Logged In

Info	10900	Microsoft Windows - Users Information : Passwords Never Expire
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10904	Microsoft Windows 'Backup Operators' Group User List
Info	10908	Microsoft Windows 'Domain Administrators' Group User List
Info	10913	Microsoft Windows - Local Users Information : Disabled Accounts
Info	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
Info	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	42822	Strict Transport Security (STS) Detection
Info	42823	Non-compliant Strict Transport Security (STS)
Info	42981	SSL Certificate Expiry - Future Expiry
Info	43111	HTTP Methods Allowed (per directory)
Info	43815	NetBIOS Multiple IP Address Enumeration
Info	43829	Kerberos Information Disclosure
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR)

		Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	66173	RDP Screenshot
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
Info	100871	Microsoft Windows SMB Versions Supported (remote check)

Anexo B Reporte Escaneo De Vulnerabilidades OPENVAS

Scan Report

November , 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scan OpenVAS". The scan started at Wed Nov 13:49:15 2017 UTC and ended at Wed Nov 15:58:51 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168. . .loc	0	2	0	24	0
Total: 1	0	2	0	24	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 26 results selected by the filtering described above. Before filtering there were 26 results.

2 Results per Host

2.1 192.168. .

Host scan start	Wed Nov	13:49:32 2017 UTC
Host scan end	Wed Nov	15:58:51 2017 UTC

Service (Port)	Threat Level
general/tcp	Medium
135/tcp	Medium
general/tcp	Log
3389/tcp	Log
3268/tcp	Log
53/tcp	Log
general/CPE-T	Log
139/tcp	Log
general/SMBClient	Log
80/tcp	Log
135/tcp	Log
88/tcp	Log
445/tcp	Log
389/tcp	Log

2.1.1 Medium general/tcp

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details:TCP Sequence Number Approximation Reset Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: $Revision: 5912 $

References
CVE: CVE-2004-0230
BID:10183
Other:
URL:http://xforce.iss.net/xforce/xfdb/15886
URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

[return to 192.168.]

2.1.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49153]
     Annotation: Wcm Service
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
     Annotation: IdSegSrv service
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
     Annotation: Proxy Manager provider server endpoint
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.      [49154]
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [49154]
      Annotation: IKE/Authip API
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [49154]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [49154]
      Annotation: Adh APIs
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [49154]
      Annotation: Impl friendly name
Port: 50301/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Annotation: KeyIso
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Annotation: Impl friendly name
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.      [50301]
      Annotation: MS NT Directory DRS Interface
Port: 50304/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_http:192.168.      [50304]
      Annotation: RemoteAccessCheck
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_http:192.168.      [50304]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_http:192.168.      [50304]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_http:192.168.      [50304]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_http:192.168.      [50304]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_http:192.168.      [50304]
      Annotation: MS NT Directory DRS Interface
Port: 50305/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.      [50305]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [50305]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [50305]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.      [50305]
      Annotation: KeyIso
Port: 5040/tcp
      UUID: 1a927394-352e-4553-ae3f-7cf4aafca620, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [5040]
Port: 51055/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [51055]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.      [51055]
      Named pipe : spoolss
```

... continues on next page ...

... continued from previous page ...

```
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51055]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51055]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51055]
Port: 51075/tcp
     UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51075]
     Annotation: PERFMON SERVICE
     UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51075]
     Annotation: NtFrs API
     UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51075]
     Annotation: NtFrs Service
Port: 51084/tcp
     UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51084]
     UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51084]
Port: 51095/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:192.168.     [51095]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
Port: 51136/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.     [51136]
Port: 51137/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.     [51137]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

[return to 192.168.]

2.1.3 Log general/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result
OpenVAS cannot reach any of the previously open ports of the remote
host at the end of its scan.
This might be an availability problem related which might be
due to the following reasons :
- The remote host is now down, either because a user turned it
off during the scan
- A network outage has been experienced during the scan, and the remote
network cannot be reached from the OpenVAS server any more
- This OpenVAS server has been blacklisted by the system administrator
or by automatic intrusion detection/prevention systems which have detected the
vulnerability assessment.
In any case, the audit of the remote host might be incomplete and may need to
be done again

Log Method
Details:Check open ports
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: $Revision: 5348 $

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informations which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to openvas-plugins@wald.intevation.org.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Best matching OS:
OS: Windows Server 2012 R2 Standard 9600
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows Server 2012
↪R2 Standard 9600; SMB String: Windows Server 2012 R2 Standard 6.3
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Microsoft Windows Server 2012 R2
CPE: cpe:/o:microsoft:windows_server_2012:r2
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Microsoft-IIS/8.5
OS: Microsoft Windows 8.1
CPE: cpe:/o:microsoft:windows_8.1
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Microsoft-IIS/8.5
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
OS: HP JetDirect
CPE: cpe:/h:hp:jetdirect
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to openvas-plugins@wald.intevation.org:
Banner: OS String: Windows Server 2012 R2 Standard 9600; SMB String: Windows Ser
↪ver 2012 R2 Standard 6.3
Identified from: SMB NativeLanMan on port 445/tcp
Banner: # Nmap 7.60 scan initiated Wed Nov 15 13:59:23 2017 as: nmap -T3 -n -Pn
↪-sV -oN /tmp/nmap-192.168.     -1018935048 -O --osscan-limit -p 3389,3269,3268
↪,636,593,464,389,135,88,80,53,21,22,25,443,19955,27051,32880 192.168.
Nmap scan report for 192.168
Host is up (0.017s latency).
PORT      STATE  SERVICE      VERSION
21/tcp    closed ftp
22/tcp    closed ssh
25/tcp    closed smtp
53/tcp    open   domain?
80/tcp    open   http         Microsoft IIS httpd 8.5
88/tcp    open   kerberos-sec Microsoft Windows Kerberos (server time: 2017-11-1
↪5 13:59:35Z)
135/tcp   open   msrpc        Microsoft Windows RPC
```

... continues on next page ...

... continued from previous page ...

```
389/tcp   open   ldap         Microsoft Windows Active Directory LDAP (Domain:
↪             .loc, Site:          )
443/tcp   closed https
464/tcp   open   kpasswd5?
593/tcp   open   ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open   tcpwrapped
3268/tcp  open   ldap         Microsoft Windows Active Directory LDAP (Domain:
↪             .loc, Site:          )
3269/tcp  open   tcpwrapped
3389/tcp  open   ssl          Microsoft SChannel TLS
19955/tcp closed unknown
27051/tcp closed unknown
32880/tcp closed unknown
*** unknown fingerprints replaced ***
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (
↪93%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host:         ; OS: Windows; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https
↪://nmap.org/submit/ .
# Nmap done at Wed Nov    14:01:49 2017 -- 1 IP address (1 host up) scanned in 1
↪49.55 seconds
Identified from: Nmap TCP/IP fingerprinting
```

Log Method
Details:OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 7600 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 10.0.2.15 to 192.168.     :
10.0.2.15
192.168.
```

Solution

... continues on next page ...

... continued from previous page ...

Block unwanted packets from escaping your network.

Log Method
Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 7278 $

[return to 192.168.]

2.1.4 Log 3389/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A TLScustom server answered on this port

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 6821 $

[return to 192.168.]

2.1.5 Log 3268/tcp

Log (CVSS: 0.0)
NVT: LDAP Detection

Summary
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.

Vulnerability Detection Result
The LDAP Server supports LDAPv3.

Log Method
Details:LDAP Detection

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.100082
Version used: $Revision: 5230 $

[return to 192.168.]

2.1.6 Log 53/tcp

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary
A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details:DNS Server Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: $Revision: 6786 $

[return to 192.168]

2.1.7 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
192.168. |cpe:/a:microsoft:iis:8.5
192.168. |cpe:/o:microsoft:windows

Log Method
Details:CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 5458 $

[return to 192.168.]

2.1.8 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
`A SMB server is running on this port`

Log Method
Details:`SMB/CIFS Server Detection`
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: `$Revision: 4261 $`

[return to 192.168.]

2.1.9 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script tests the remote host SMB Functions with the 'smbclient' tool.

Vulnerability Detection Result
`Error getting SMB-Data -> CONNECTION TO 192.168. FAILED (ERROR NT_STATUS_HO`
`↪ST_UNREACHABLE)`

Log Method
Details:`SMB Test with 'smbclient'`
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: `$Revision: 6841 $`

[return to 192.168.]

2.1.10 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

... continues on next page ...

... continued from previous page ...

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning' and 'Enable generic web application scanning' within the 'Global variable settings' of the scan config in use
If you think any of these are wrong please report openvas-plugins@wald.intevation.org

Vulnerability Detection Result

```
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The following directories were used for CGI scanning:
http://                         .loc/
http://                         .loc/cgi-bin
http://                         .loc/scripts
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details:CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 7428 $

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result

```
This are the directories/files found with brute force:
http://                         .loc:80/
```

Log Method
Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: $Revision: 6841 $

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result
```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method
Details:HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: $Revision: 7484 $

References
```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
```
The remote web server type is :
Microsoft-IIS/8.5
```

Solution
Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details:HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 6760 $

Log (CVSS: 0.0)
NVT: Microsoft IIS Webserver Version Detection

Summary
This script detects the installed MS IIS Webserver and sets the result in KB

Vulnerability Detection Result

```
Detected Microsoft IIS Webserver
Version:  8.5
Location: 80/tcp
CPE:      cpe:/a:microsoft:iis:8.5
Concluded from version/product identification result:
IIS/8.5
```

Log Method
Details:Microsoft IIS Webserver Version Detection
OID:1.3.6.1.4.1.25623.1.0.900710
Version used: $Revision: 6065 $

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 192.168.     :80
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 7155 $

Log (CVSS: 0.0)
NVT: Services

... continues on next page ...

... continued from previous page ...

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 6821 $`

Log (CVSS: 0.0)
NVT: Windows SharePoint Services detection

Summary
The remote host is running Windows SharePoint Services. Microsoft SharePoint products and technologies include browser-based collaboration and a document-management platform. These can be used to host web sites that access shared workspaces and documents from a browser.

Vulnerability Detection Result
```
Detected Microsoft-IIS
Version:  8.5
Location: /
CPE:      cpe:/a:microsoft:iis:8.5
Concluded from version/product identification result:
8.5
```

Solution
It's recommended to allow connection to this host only from trusted hosts or networks.

Log Method
Details:`Windows SharePoint Services detection`
OID:1.3.6.1.4.1.25623.1.0.101018
Version used: `$Revision: 6760 $`

Log (CVSS: 0.0)
NVT: Windows SharePoint Services detection

Summary
The remote host is running Windows SharePoint Services. Microsoft SharePoint products and technologies include browser-based collaboration and a document-management platform. These can be used to host web sites that access shared workspaces and documents from a browser.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Server: Microsoft-IIS/8.5
Operating System Type: Windows Server 2012 R2 / Windows 8.1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET

Solution
It's recommended to allow connection to this host only from trusted hosts or networks.

Log Method
Details:Windows SharePoint Services detection
OID:1.3.6.1.4.1.25623.1.0.101018
Version used: $Revision: 6760 $

[return to 192.168.]

2.1.11 Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

Vulnerability Detection Result
A DCE endpoint resolution service seems to be running on this port.

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this port.

Log Method
Details:DCE/RPC and MSRPC Services Enumeration
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: $Revision: 7268 $

[return to 192.168.]

2.1.12 Log 88/tcp

Log (CVSS: 0.0)
NVT: Kerberos Detection (TCP)

Summary
The script sends a connection request to detect a running kerberos server.

Vulnerability Detection Result
```
A Kerberos Server is running at this port.
Realm:                .LOC
Server time: 2017-11-   14:01:43
```

Log Method
Details:Kerberos Detection (TCP)
OID:1.3.6.1.4.1.25623.1.0.103854
Version used: $Revision: 4822 $

[return to 192.168.]

2.1.13 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Detected SMB workgroup:
Detected SMB server: Windows Server 2012 R2 Standard 6.3
Detected OS: Windows Server 2012 R2 Standard 9600
```

Log Method
Details:SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: $Revision: 7732 $

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
SMB Protocol not enabled on remote target

Log Method
Details:SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: $Revision: 5438 $

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects wether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A CIFS server is running on this port

Log Method
Details:SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 4261 $

[return to 192.168.]

2.1.14 Log 389/tcp

Log (CVSS: 0.0)
NVT: LDAP Detection

Summary
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.

Vulnerability Detection Result
The LDAP Server supports LDAPv3.

Log Method
Details:LDAP Detection
OID:1.3.6.1.4.1.25623.1.0.100082
Version used: $Revision: 5230 $

[return to 192.168.]

Anexo C Reporte Escaneo a Puertos TCP con NMAP

root@Scan:~# nmap -sS -sV 192.168.XXX.XXX

Starting Nmap 7.60 (https://nmap.org) at 2017-11-16 09:42 -05
Nmap scan report for XXXXXXXX.XXXXXXXXXXXX.loc (192.168.XXX.XXX)
Host is up (1.0s latency).
Not shown: 983 closed ports
PORT STATE SERVICE VERSION
53/tcp open domain Microsoft DNS
80/tcp open http Microsoft IIS httpd 8.5
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2017-11-16 14:42:47Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: XXXXXXXXXXX.loc, Site: XXX-XXXXX)
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: XXX-XXXXX)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: XXXXXXXXXXX.loc, Site: XXX-XXXXX)
3269/tcp open tcpwrapped
3389/tcp open ssl Microsoft SChannel TLS
14000/tcp open scotty-ft?
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3389-TCP:V=7.60%I=7%D=11/16%Time=5A0DA3EC%P=x86_64-pc-linux-gnu%r(T
SF:LSSessionReq,362,"\x16\x03\x03\x03\]\x02\0\0M\x03\x03Z\r\xa3\xe7\xeb\x9
SF:b\xcc\xfc\xdf\x8f:\x8b\xcc\xb7\x95\|L\x9d\xa1\xb3f`\x187\x83\x82\xe4\xf
SF:1:u\xca6\x20y\x15\0\0I\xfa\xb9\x19\xfeIpX\x86\x14\xfc\xeb\xba\xeb\xc7\x
SF:08\xa7\x11\xf4\xf6\xe7h\xa5\x82\x8aa\xf8\]\0/\0\0\x05\xff\x01\0\x01\0\x
SF:0b\0\x03\x04\0\x03\x01\0\x02\xfe0\x82\x02\xfa0\x82\x01\xe2\xa0\x03\x02\
SF:x01\x02\x02\x10\x15\x11<\xab\xb3\xd7&\xaaH*\xa1#\x9f\xc2\x16b0\r\x06\t
SF:*\x86H\x86\xf7\r\x01\x01\x05\x05\x000&1\$0\"\x06\x03U\x04\x03\x13\x1bC
SF:GRVALLE\.XXXXXXXXXXX\.loc0\x1e\x17\r170513000131Z\x17\r171112000131Z
SF:0&1\$0\"\x06\x03U\x04\x03\x13\x1bXXXXXXXX\.XXXXXXXXXXX\.loc0\x82\x01
SF:\"0\r\x06\t*\x86H\x86\xf7\r\x01\x01\x01\x05\0\x03\x82\x01\x0f\x000\x82

SF:\x01\n\x02\x82\x01\x01\0\xc6\xf0Xr\xee}\xde\x95r\x02\x97\xb4\xd4FT\x16\
SF:xcaRL\x94\xbd\xe4\xa0\xc0\xaa@\x05\xcf\x8e9\x95>\xdf\x93L\xb6\x86\xa3\x
SF:bc\x11fkU\xd6\x16\xe4\xd2\n\x810\xc84zly\xd2\x91\xfa\xea\xeb\x89\x96\"w
SF:'\xd8\x97\xfc\x0fP\xc6\xf5\xb1\0\(6\x19\x9e\xe1\xcc\xea\x8d\x03n\xe3\x1
SF:d}b\x19\xb8~\+\x05d!j\xb5\xc8\xc1\x8eaF\x90bn\xc5\xde\xf1D\xb6\xa7\xdf\
SF:xec\\\xda\xe6*\x1a\xce{l\xf9R\xc9\xf7\x8c\xd4\xafY\x01w\xe3\x8d\x99\[\
SF:)\xb0\n\x82\x8c\xcd\x98'\xa4\xcd\xc1_\x1b\x01\x185\x93\xae,\x9d\x885\xa
SF:fU\.\xec\xcd\xa1\x95\xa0\x11\x05\x82\xd1}\x85\xb9\xb3\x13\xedI\xbcb\xdc
SF:\xaf\xb5\xf3A,\x83\xbbjp*F\xc5\[\x03\x89\x1f\x8d\x85\xea\xe61\x1f\xb5J
SF:\n\xe9\n7\r\xcbE\xd2\xc8\x94qX\x8c\xf0\x9d\xb9\x02\xa1\xfb\x1dbWr\r{SO\
SF:x9f\x0b\xa1\x08\xee\xfc\xda\x96\xe0\xb6\"\x14\]\xcf\xcf\xbb\x117\x0c\xe
SF:9\xd21\x88\x06\x8c\xc7\x02\x03\x01\0\x01\xa3\$0\"0\x13\x06\x03U\x1d%\x0
SF:4\x0c0\n\x06\x08\+\x06\x01\x05\x05\x07\x03\x010\x0b\x06\x03U\x1d\x0f\x0
SF:4\x04\x03\x02\x0400\r\x06\t*\x86H\x86\xf7\r\x01\x01\x05\x05\0\x03\x82\
SF:x01\x01\0\xb23hfid\xab\xc3O\xae\xcb\x06\)\xd0\$\x1a\x1a;\xfd\xc3>\?f\(\
SF:xf1Jz\xdajX\|V\x98V\x1ac\x9dq\0\xebs\xd3\x8b\x07\xaa\xf0\xd2!J\xd5\x9d\
SF:$\x88\x16\?I\xf6\x01\xb6\xed\xe7\0\x03\x1c\x7f\x17~D\xbe\xc4\xc2<\xe9\x
SF:abH\xa9\xf7V\xd3\xff7\x96\+\x99\xae\x93\x17\x8dcX\x12\xab\xf1\xa7\x7f\x
SF:a9\x98M9\xb9\x9b\xbb\?\)Y\xb6'\x86\xcd\x98\xfa\r\xc8\xb4\xa3\xc2M\x08F\
SF:xfd\xbcs\x1au\xb8\x08\x8d\x03\xcb/&\xaa\xe5\xbb;K\x0c\x1e%hg\x94H\xbc\x
SF:81qY\?\x04\xdd\xeeb\|\x87\xc0\x06\x83\xd3\xcc\xb0N%\xb1\xa0\xac\xd4\^\x
SF:1e\x96\x07\x02\|\x13{\xbf\xdf\xa7\xb7\x8b\x8f\xbf\xa8\xc50R\xe4\xc2\xed
SF:3>!\xeb\xbb\x0c\xb4\xed\xe9\(\xf3\xee\xa3iG\x04r\xc1\r#\xfa1S\[K\xf9\xe
SF:8!vH\x03\x80\x07\xb7y>\xcej\[\xaa\xb0*\xe5d%/\xef\x14\xc7\x15\x823\xe1
SF:\xc70\xedp\x8cG\xa9P2\xa6\x8e\x08s`r\x0e\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port14000-TCP:V=7.60%I=7%D=11/16%Time=5A0DA3F6%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,91A,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:
SF:\x20text/xml;\x20charset=utf-8\r\nContent-Length:\x202218\r\nConnection
SF::\x20close\r\n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"UTF-8\"\?>\n
SF:<SOAP-ENV:Envelope\x20xmlns:SOAP-ENV=\"http://schemas\.xmlsoap\.org/soa
SF:p/envelope/\"\x20xmlns:SOAP-ENC=\"http://schemas\.xmlsoap\.org/soap/enc
SF:oding/\"\x20xmlns:xsi=\"http://www\.w3\.org/2001/XMLSchema-instance\"\x
SF:20xmlns:xsd=\"http://www\.w3\.org/2001/XMLSchema\"\x20xmlns:ns=\"urn:pe
SF:rson\"\x20xmlns:param=\"http://tempuri\"\x20xmlns:aklwngt=\"http://temp
SF:uri\.org/aklwngt\.xsd\"\x20xmlns:wusTypes=\"http://microsoft\.com/wsdl/
SF:types/\"\x20xmlns:wusClientSoap=\"http://www\.microsoft\.com/SoftwareDi
SF:stribution/Server/ClientWebService/ClientSoap\"\x20xmlns:wusClientWebSe
SF:rvice=\"http://www\.microsoft\.com/SoftwareDistribution/Server/ClientWe
SF:bService\"\x20xmlns:wusClientSoap12=\"http://www\.microsoft\.com/Softwa
SF:reDistribution/Server/ClientWebService/ClientSoap12\"\x20xmlns:wusDssAu
SF:thWebService=\"http://www\.microsoft\.com/Soft")%r(FourOhFourRequest,91
SF:A,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/xml;
SF:\x20charset=utf-8\r\nContent-Length:\x202218\r\nConnection:\x20close\r\
SF:n\r\n<\?xml\x20version=\"1\.0\"\x20encoding=\"UTF-8\"\?>\n<SOAP-ENV:Env
SF:elope\x20xmlns:SOAP-ENV=\"http://schemas\.xmlsoap\.org/soap/envelope/\"
SF:\x20xmlns:SOAP-ENC=\"http://schemas\.xmlsoap\.org/soap/encoding/\"\x20x

SF:mlns:xsi=\"http://www\.w3\.org/2001/XMLSchema-instance\"\x20xmlns:xsd=\
SF:"http://www\.w3\.org/2001/XMLSchema\"\x20xmlns:ns=\"urn:person\"\x20xml
SF:ns:param=\"http://tempuri\"\x20xmlns:aklwngt=\"http://tempuri\.org/aklw
SF:ngt\.xsd\"\x20xmlns:wusTypes=\"http://microsoft\.com/wsdl/types/\"\x20x
SF:mlns:wusClientSoap=\"http://www\.microsoft\.com/SoftwareDistribution/Se
SF:rver/ClientWebService/ClientSoap\"\x20xmlns:wusClientWebService=\"http:
SF://www\.microsoft\.com/SoftwareDistribution/Server/ClientWebService\"\x2
SF:0xmlns:wusClientSoap12=\"http://www\.microsoft\.com/SoftwareDistributio
SF:n/Server/ClientWebService/ClientSoap12\"\x20xmlns:wusDssAuthWebService=
SF:\"http://www\.microsoft\.com/Soft");
Service Info: Host: XXXXXXXX; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.40 seconds
root@Scan:~#

Anexo D Reporte Escaneo a Puertos UDP con NMAP

```
root@Scan:~# nmap -sU 192.168.XXX.XXX

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-16 15:11 -05
Nmap scan report for XXXXXXXX.XXXXXXXXXXXX.loc (192.168.XXX.XXX)
Host is up (0.0014s latency).
Not shown: 907 filtered ports, 65 open|filtered ports
PORT      STATE SERVICE
123/udp   open  ntp
137/udp   open  netbios-ns
389/udp   open  ldap
49160/udp open  unknown
49169/udp open  unknown
49171/udp open  unknown
49172/udp open  unknown
49173/udp open  unknown
49174/udp open  unknown
49177/udp open  unknown
49185/udp open  unknown
49186/udp open  unknown
49193/udp open  unknown
49196/udp open  unknown
49197/udp open  unknown
49198/udp open  unknown
49200/udp open  unknown
49202/udp open  unknown
49205/udp open  unknown
49209/udp open  unknown
49210/udp open  unknown
49222/udp open  unknown
49226/udp open  unknown
49306/udp open  unknown
49393/udp open  unknown
64513/udp open  unknown
64590/udp open  unknown
65024/udp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1722.58 seconds
root@Scan:~#
```

Anexo E Reporte Escaneo de Vulnerabilidades con Microsoft Baseline Security Analyzer

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	
IP address:	192.168. .
Security report name:	- (22-11-2017 8-15 a. m.)
Scan date:	22/11/2017 8:15 a. m.
Catalog synchronization date:	2017-11-11T01:56:02Z
Security update catalog:	Microsoft Update (offline)

Security Updates

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing.

Security Updates

Score	ID	Description	Maximum Severity
Missing	MS11-025	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Important
Missing	MS11-025	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	Important

Windows Security Updates	7 security updates are missing. 1 service packs or update rollups are missing.	

Security Updates

Score	ID	Description	Maximum Severity
Missing	MS14-040	Security Update for Windows Server 2012 R2 (KB2973408) without KB2919355	Important
Missing	2975625	Security Update for Windows Server 2012 R2 (KB2975625) without KB2919355	
Missing	MS14-031	Security Update for Windows Server 2012 R2 (KB2961858) without KB2919355	Important
Missing	MS16-100	Security Update for Windows Server 2012 R2 (KB3172729)	Important
Missing	MS14-018	Windows Server 2012 R2 Update (KB2919355)	Critical
Missing	MS14-036	Security Update for Windows Server 2012 R2 (KB2965161) without KB2919355	Critical
Missing	MS14-039	Security Update for Windows Server 2012 R2 (KB2973906) without KB2919355	Important

Update Rollups and Service Packs

Score	ID	Description
Missing	890830	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - November 2017 (KB890830)

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	2862152	Security Update for Windows Server 2012 R2 (KB2862152)	
Installed	MS14-019	Security Update for Windows Server 2012 R2 (KB2922229)	Important
Installed	MS13-098	Security Update for Windows Server 2012 R2 (KB2893294)	Critical
Installed	MS13-099	Security Update for Windows Server 2012 R2 (KB2892074)	Critical
Installed	2920189	Security Update for Windows Server 2012 R2 (KB2920189)	
Installed	890830	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)	
Installed	MS13-095	Security Update for Windows Server 2012 R2 (KB2868626)	Important
Installed	2961908	Security Update for Windows Server 2012 R2 (KB2961908) without KB2919355	
Installed	MS14-026	Security Update for Microsoft .NET Framework 4.5.1 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2931366)	Important
Installed	4019111	May, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4019111)	Important
Installed	MS14-025	Security Update for Windows Server 2012 R2 (KB2961899) without KB2919355	Important
Installed	MS14-007	Security Update for Windows Server 2012 R2 (KB2912390)	Critical

SQL Server Security Updates	No security updates are missing.	

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	Some user accounts (630 of 4951) have non-expiring passwords. **User**

Administrators More than 2 Administrators were found on this computer.
User

Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted.	
Windows Firewall	Windows Firewall is managed through Group Policy on this computer. Windows Firewall is disabled and has exceptions configured.	

Connection Name	Firewall	Exceptions
All Connections	Off	Ports, Programs, Services
Ethernet	Off*	Ports*, Programs*, Services*
Ethernet 2	Off*	Ports*, Programs*, Services*
Ethernet 3	Off*	Ports*, Programs*, Services*
Ethernet 4	Off*	Ports*, Programs*, Services*

File System	All hard drives (2) are using the NTFS file system.	

Drive Letter	File System
C:	NTFS
E:	NTFS

Guest Account	The Guest account is disabled on this computer.
Autologon	Autologon is not configured on this computer.
Restrict Anonymous	Computer is properly restricting anonymous access.
Automatic Updates	Updates are automatically downloaded and installed on this computer.
Local Account Password Test	Password checks are not performed on a domain controller.

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 8.1.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such logon and logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	21 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
F$	F:\	Admin Share	Directory ACL can not read.

	Services	Some potentially unnecessary services are installed.	
		Service	**State**
		Servicio de publicación World Wide Web	Running

Internet Information Services (IIS) Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Sample Applications	IIS sample applications are not installed.
	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
	Parent Paths	Parent paths are not enabled.
	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.
	IIS Lockdown Tool	The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations running IIS 6.0.

Additional System Information

Score	Issue	Result
	Domain Controller Test	IIS is running on a primary or backup domain controller.
	IIS Logging Enabled	All web and FTP sites are using the recommended logging options.

SQL Server Scan Results: Instance MSWIN8.SQLWID

Administrative Vulnerabilities

Score	Issue	Result

Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.	
SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to Windows Only.	
CmdExec role	CmdExec is restricted to sysadmin only.	
Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.	
Folder Permissions	**Instance**	**Folder** / **User**
	MSWIN8.SQLWID	Internal error. / -
Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.	
Sysadmin role members	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Guest Account	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Sysadmins	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Password Policy	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
SSIS Roles	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Sysdtslog	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones do not have secure settings for some users.

User	Zone	Level	Recommended Level
\williams.avila	Internet	High	High

Setting	Current	Recommended
Download signed ActiveX controls	Prompt	Disable
File download	Enable	Disable
Submit nonencrypted form data	Enable	Prompt

Macro Security	No supported Microsoft Office products are installed.	