ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN CASO DE ESTUDIO

MARIO ANDRÉS CARVAJAL AVILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN CASO DE ESTUDIO

MARIO ANDRES CARVAJAL AVILA

Trabajo de grado para optar el título de
Especialista en Seguridad Informática

Esp. Ing. Freddy Enrique Acosta
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá DC, Diciembre 23 del 2018

Ha sido un camino que he recorrido con esfuerzos y sacrificios para llegar a cumplir una gran etapa en la formación personal y profesional en mi vida, Doy gracias de todo corazón principalmente a Dios por darme fuerzas y sabiduría para seguir adelante,

A mi querida Esposa, Natalia Del Pilar Barón Gómez por su apoyo incondicional, a mis apreciados Padres, Martha Isabel Avila de Carvajal y José Mario Carvajal Alarcón por brindarme ese amor tan único con el apoyo incondicional y sacrificio para que se hiciera realidad mi proyecto de vida
A mi hermano Diego Fernando Carvajal Avila, por acompañarme y brindarme el apoyo en todo momento

A mis Familiares, Docentes, Amigos, compañeros y a todas las personas que han estado presente en este tiempo de formación.

Mario Andrés Carvajal Avila

AGRADECIMIENTOS

Mario Andrés Carvajal Avila expresa su agradecimiento:

A la Subdirectora de Tecnologías Leydy Yohana Pineda Afanador, Al Oficial de seguridad Ing. Héctor Andrés Mafla y la organización caso de estudio por ofrecerme la oportunidad de desarrollar mi proyecto aplicativo.

Al Coordinador de Infraestructura Marco Guerrero y los Ingenieros de Infraestructura por brindarme una guía adecuada y precisa, por el apoyo incondicional en todo el transcurso del proyecto.

Al Director de Proyecto Esp. Ing Freddy Acosta por brindarme el apoyo y sus conocimientos profesionales, a la Universidad Nacional Abierta y a Distancia, los Docentes, y compañeros que son parte de este gran proceso de formación y aprendizaje.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTAS DE FIGURAS

Pág.

GLOSARIO

Vulnerabilidad: Debilidad de un elemento tecnológico que permite un comportamiento no deseado, que son generados por fallos de diseño, errores de configuración o carencia de procedimientos[1].

CVE: Vulnerabilidades Comunes y Expuestas, comprende una lista de nombres estandarizados para vulnerabilidad, facilitando la búsqueda de información en la base de datos de vulnerabilidades[2].

Exploit: Fragmento de código desarrollado para aprovechar una vulnerabilidad especifica.

Severidad crítica: Vulnerabilidad de alto grado de impacto.

Severidad alta: Vulnerabilidades que requieren atención inmediata.

Severidad media: Vulnerabilidades que requieren atención de tipo estándar.

Severidad baja: Vulnerabilidades que requieren atención después de atender eventos o incidentes con severidad alta y/o media.

Malware: Software Malicioso o malintencionado diseñado para causar efectos no deseados en un dispositivo[3].

CBC: Cifrado de bloques cambiante.

Hash: Algoritmo matemático usado para comprobar la autenticidad de un archivo o un dato.

Man-In-The-Middle (Mitm): Ataque que permite a un atacante leer información, ubicándose en medio del origen y el destino de la información.

AES: Estándar avanzado de encriptación.

Arcfour: Algoritmo de cifrado también conocido como RC4.[4]

Mitigación: Se refiere atenuar algo negativo, como riesgos informáticos.

---

[1] AMENAZA VS VULNERABILIDADES. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[2] GGI LAN GUARD 12. Vulnerabilidades y exposiciones comunes (CVE). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm

[3] SYMANTEC CORPORATION. ¿En qué consiste el malware?). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.websecurity.symantec.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

[4] NULLPROGRAM. The Arcfour Stream Cipher.). [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://nullprogram.com/blog/2008/08/09/

El presente proyecto aplicativo tiene como finalidad explorar y aplicar las pruebas de vulnerabilidades mediante la utilización de herramientas, procesos y metodología de pruebas de vulnerabilidades. Se ha querido revisar y explorar las vulnerabilidades presentes en los host más críticos (servidores Físicos y máquinas virtuales) de la organización, con el fin de mitigar, solucionar, beneficiar y optimizar los recursos en los procesos que ejecuta la organización, manteniendo confidencialidad y seguridad de la información.

En la organización caso de estudio se ha evidenciado ataques e intentos de accesos no autorizados, que han sido validados mediante herramientas de seguridad perimetral como el firewall, Analyzer y Sandbox, motivo por el cual es necesario aplicar el plan de pruebas y mitigación de vulnerabilidades sobre los host más críticos (servidores y máquinas virtuales) perteneciente al empresa caso de estudio.

Para el desarrollo de la práctica se realizara mediante pruebas utilizadas de manera ordenada con la metodología de Ética Hacking para describir el proceso del desarrollo del proceso del plan de pruebas y mitigación de vulnerabilidades, además se manipulara herramientas de pen test y análisis que serán necesarios para realizar el procedimiento, así como Kali Linux, Nmap, Nessus.

Los resultados del procedimiento en aplicar el escaneo y análisis de vulnerabilidades en la organización se detallara mediante un informe área de tecnología y cómputo de la organización caso de estudio la lista de las vulnerabilidades encontradas y certificadas mediante CVE (Common Vulnerabilities and Exposures), adicionalmente este documento se proporcionará una lista de recomendaciones que se deben aplicar e informando los resultados obtenidos antes y después, con el propósito de mitigar con soluciones que han sido detallados con las personas involucradas en área de tecnología y cómputo y aplicativos que operan los host más críticos de la organización caso estudio .

PALABRAS CLAVES: NMAP, KALI LINUX, NESSUS, HOST, VULNERABILIDADES, SEVERIDADES

The purpose of this application project is to explore and apply vulnerability testing through the use of tools, processes and vulnerability testing methodology. It has been wanted to review and explore the vulnerabilities present in the most critical hosts (physical servers and virtual machines) of the organization, in order to mitigate, solve, benefit and optimize the resources in the processes that the organization runs, maintaining confidentiality and security of information.

In the organization case study has evidenced attacks and attempts of unauthorized access, which have been validated by perimeter security tools such as firewall, Analyzer and Sandbox, which is why it is necessary to apply the test plan and mitigation of vulnerabilities on the most critical hosts (servers and virtual machines) belonging to the company case study.

For the development of the practice will be performed through tests used in an orderly manner with the methodology of Ethics Hacking to describe the process of developing the process of testing plan and mitigation of vulnerabilities, also manipulated pen test tools and analysis that will be necessary to perform the procedure, as well as Kali Linux, Nmap, Nessus.

The results of the procedure in applying the scanning and analysis of vulnerabilities in the organization will be detailed through a report area of technology and computation of the organization case study the list of vulnerabilities found and certified by CVE (Common Vulnerabilities and Exposures), additionally this document will provide a list of recommendations to be applied and reporting the results obtained before and after, in order to mitigate with solutions that have been detailed with the people involved in the area of technology and computation and applications that operate the most critical hosts of the organization case study.

KEYWORDS: NMAP, KALI LINUX, NESSUS, HOST, VULNERABILITIES, SEVERIDADES

INTRODUCCIÓN

La información y los sistemas de las organizaciones son víctima de ataques que pueden ocurrir sobre aplicaciones o servicios expuestos, y otros son aprovechados por vulnerabilidades que se presenta en dicho sistemas.

"De este modo comienza con la planeación, la cual se encarga de valorar, analizar, y proyectar los di referentes riesgos que se encuentre presente en el ambiente empresarial. De acuerdo con este plan, se debe implementar políticas de seguridad, identificando las amenazas internas y externas, teniendo en cuenta la infraestructura tecnológica que posee… luego se implementa la parte práctica, eligiendo y estableciendo arquitectura de red, en el cual se monte todos los servicios que presta la organización, asegurando cada uno de esto; llevando a cabo una auditoria de este proceso, la cual se debe seguir realizándose periódicamente"[5]

Se hace necesario realizar un análisis de vulnerabilidades para identificar aquellas brechas de seguridad a las que se encuentran expuestas tanto externa e internamente la Institución. Este análisis de vulnerabilidades se realizará mediante escaneo de puertos activos y vulnerabilidades, en donde se aplican pruebas de "pen test" que son realizadas mediante metodologías de hacking ético con el uso de software y herramientas que son primordiales para este tipo de procedimiento.

Por lo tanto " Existen metodología la cual da a conocer una seria de pasos, que abracan diferentes temas como lo son la planeación, políticas de seguridad, aseguramiento de la seguridad de la información, haciendo que un sistema permanezca cubierto y preparado ante eventualidad que puedan interrumpir el desarrollo normal de las actividades de una organización"[5]

Con el análisis se lograra disminuir y controlar los peligros existentes a los que se encuentran expuestos los host más críticos de la empresa caso de estudio, así como también conocer la situación actual de seguridad de la organización con el fin de implementar medidas preventivas y correctivas con el fin mitigar dichos riesgos y amenazas.

[5] GARZÓN, Daniel. RATKOVICH GOMES, Juan. Metodología de Análisis de Vulnerabilidades para Empresa de mediana y pequeña escala [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

1. DEFINICION DEL PROBLEMA

Se definió que se requiere mantener con seguridad todo lo que es relacionado con la información y accesos a los sistemas que pueden ser husmeados por algunos intrusos con el propósito de realizar alguna actividad ilícita e ilegal. Por tal motivo se debe satisfacer las necesidades brindando la confidencialidad, disponibilidad e integridad que permiten resguardar y proteger los datos y los sistemas donde se encuentra alojado su información considerado críticos.

El hacking Ético se ha considerado una buena práctica en aplicar procesos que conlleve a encontrar brechas de seguridad, considerados vulnerabilidades sobre algún sistema, por necesidad de la empresa caso de estudio en conocer sus debilidades de seguridad, se realizara el escaneo de puertos y vulnerabilidades, con el objetivo de entregar la respectiva información para que puedan elaborar el plan de mitigación de vulnerabilidades que será aplicado por el área de infraestructura como solución a sus problemas de seguridad, satisfaciendo la necesidad de la empresa caso de estudio.

"Con el fin de incrementar tal seguridad se hace necesario realizar un análisis de vulnerabilidades, para identificar aqueas brechas de seguridad que se encuentran expuestas"[6]

El presente proyecto aplicativo tiene como propósito mejorar, disminuir y controlar la seguridad de los host (servidores y máquinas virtuales) en los sistemas considerados más críticos, mediante la ejecución de pruebas de vulnerabilidades basados en herramientas de PenTest, teniendo en cuenta los pasos necesarios para realizar el procedimiento sin afectar ningún servicio en la institución.

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las empresas tanto el sector público como el privado priorizan la seguridad de la información, que es considerada como uno de los bienes críticos e importantes para la continuidad del negocio. Las buenas prácticas se realizan con el fin de prevenir los diferentes tipos de ataques, analizando las posibles vulnerabilidades que presenta los host que contiene información primordial de la Institución.

" Pfleeger y Ciszek (2008), exponen una metodología compuesto de cuatro pasos que pretende ayudar a las organizaciones a evaluar los activos relevantes a ser protegidos, estableciendo los potenciales atacantes y los posibles métodos para

[6] GARZÓN, Daniel. RATKOVICH GOMES, Juan. VERGARA TORRES. Alejandro. Metodología de Análisis de Vulnerabilidades para Empresa de mediana y pequeña escala. [2018] [en línea] [citado el 08 de noviembre ,2018] Disponible en internet: https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

disminuir el riesgo, sin embargo, no se precisan técnicas para evaluación de la seguridad de dichos activos".

En la organización caso de estudio, no se encuentra exento de riesgos y amenazas sobre las bases de datos y aplicativos desarrollados en la Institución, por este motivo es necesario implementar este proyecto en donde se realizara el escaneo de vulnerabilidades sobre los host más críticos (servidores y máquinas virtuales), con el objetivo de mitigar dichas amenazas y de informar las respectivas recomendaciones para que los involucrados realicen el plan de mitigación de las vulnerabilidades halladas, adicionalmente, se pretende con ello alcanzar un nivel más óptimo, mejorando y fortaleciendo la seguridad de la información a la organización caso de estudio.

"podemos mencionar que en el campo de las aplicaciones Web sobresalen NeXpose (también útil para plataformas de escritorio), acunetix, w3af, entre otros. Algunos de estos proyectos han sido examinados en trabajos de investigación (Bau et al., 2010) donde se evaluaron ocho diferentes escáneres de vulnerabilidades de aplicaciones web, con el fin de determinar su efectividad en la detección de éstas. Además, otro trabajo (Shi et al., 2010) realizó la evaluación de diferentes herramientas de seguridad, a la vez que se compararon las habilidades de las mismas" [5]

Se analizará el escaneo de algunos de los servicios de puertos y permisos de accesos que son solicitados por el usuario para el desarrollo de su labores, donde se encuentra alojada la información más importante, considerada confidencial para la institución, se considera necesario aplicar y analizar el escaneo de vulnerabilidades ya que al dar estos permisos la institución está expuesta a los accesos no autorizados por intrusos o ciberdelincuentes.

“Pese a los trabajos que han sido realizados el problema que surge de la presencia de vulnerabilidades en redes de datos, sigue causando grandes pérdidas a organizaciones e individuos en la actualidad, por esto se han desarrollado diferentes metodologías para la detección de dichas vulnerabilidades (Watanabe et al., 2010)"[7]

1.2 FORMULACION DEL PROBLEMA

¿Cómo Analizar y mitigar las vulnerabilidades que se encuentra en los Host más críticos en la organización caso de estudio?.

1.3 OBJETIVOS

1.3.1 Objetivo general

- Realizar análisis y escaneo de vulnerabilidades a la infraestructura Tecnológica de la entidad caso de estudio.

1.3.2 Objetivos específicos

- Recolección de información de los host críticos de la organización caso de estudio para monitorear y tener un control de inventario de las mismas.

- Aplicación de "Pen Test" para hallar y analizar las vulnerabilidades, usando las respectivas herramientas de seguridad informática sobre los host más críticos (Servidores físicos y máquinas virtuales) de la organización caso de estudio.

- Análisis de vulnerabilidades identificadas, teniendo en cuenta su nivel de severidad en los host críticos de la organización caso de estudio.

- Informe de vulnerabilidades halladas, especificando las recomendaciones necesarias para concluir con las vulnerabilidades de la empresa caso de estudio.

1.4 JUSTIFICACION

En la organización caso de estudio, es importante escanear las vulnerabilidades en los host más críticos como en la base de datos, donde se encuentran alojados la información más importante y aplicaciones, afectando el desarrollo y procesos de usuarios en la Institución.

"Por tal motivo se creó el área de seguridad informática, área que se encarga de brindar protección en los diferentes sectores de la empresa. Esta se fundamenta en cinco principios básicos: confidencialidad, disponibilidad, integridad, audibilidad y no repudio, pero se debe tener en cuenta que no solo con esto principios se garantiza una seguridad efectiva, ya que la forma en que estos principios tengan efectos en pro de la organización es mediante la implantación de controles o mecanismo de seguridad basados en las políticas generales de la empresa, particularmente en las políticas y procedimientos de seguridad, con lo que se busca minimizar las vulnerabilidades expuestas y aumentar la seguridad de la información."[7]

[7] GARZÓN, Daniel. RATKOVICH GOMES, Juan. VERGARA TORRES. Alejandro. Metodología de Análisis de Vulnerabilidades para Empresa de mediana y pequeña escala. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Se hace necesario realizar este proyecto aplicativo en la organización caso de estudio, con la finalidad de evaluar la seguridad en la que se encuentra la institución y con el objetivo de mitigar las amenazas y riesgos a los que están expuestos los host más críticos, lo cual permitirá entregar la información para que se plantee un plan de mitigación de vulnerabilidades para mantener un sistema de gestión de la seguridad de la información (SGSI) más confiable.

“De este modo, el estudio de estas vulnerabilidades debe abarcar varios frente de seguridad, reduciendo al mínimo la efectividad de los ataques que pueden provechar las mismas” [7]

El presente proyecto aplicativo se basará en la utilización de software "pen test" con el que se realizara el respectivo escaneo de vulnerabilidades y puertos que se ejecutara en una maquina con sistema operativo Kali Linux.

“Así mismo se deben identificar y mitigar los riesgos a los que se encuentre expuesta la empresa, de tal modo que cada uno identifique, mitigue cada uno de los mismos, basados en la necesidades y requerimiento de la empresa”.[7]

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcance

El presente proyecto se encuentra entre los proyectos de seguridad Informática y lo que se pretenden es realizar el escaneo y análisis de vulnerabilidades a los host más críticos, con el fin de brindar la información necesaria, teniendo en cuenta los resultados obtenidos, para que la organización caso de estudio pueda desarrollar el plan de mitigación de riesgos y amenazas.

Se tendrá en cuenta las severidades Críticas medias y Altas como lo solicita el oficial de seguridad de la información de la organización caso de estudio.

1.5.2 Limitaciones

Es conveniente resaltar que el desarrollo del presente proyecto aplicativo no abarcara temas como los que se definen a continuación:

- No se publicara el nombre de la entidad, direccionamiento IP, nombre reales de los host por seguridad confidencial

- No se implementara el plan de mitigación de vulnerabilidades encontradas en los análisis obtenidos mediante el proceso de escaneo.

- No se realizara la explotación de las vulnerabilidades escaneadas.
- Solo se aplicara la metodología descrita en los objetivos, como son el escaneo de puertos, vulnerabilidades y realización de informe que será entregado a la organización caso de estudio.

1.6 DISEÑO METODOLÓGICO

1.6.1 Unidad de Análisis.

Para realizar el estudio de análisis y escaneo de vulnerabilidades se tomara como referente a la organización caso de estudio.

1.6.2 Población y muestra

1.6.2.1 Población

La población está conformada por las 40 Host (servidores físicos y máquinas virtuales) que se encuentra en el área de tecnología y cómputo perteneciente a la organización caso de estudio

1.6.2.2 Muestra

La muestra se obtuvo de acuerdo a la información recolectada en el área de tecnología y computo de acuerdo a los servicios que se encuentra más expuestos a vulnerabilidades, siendo esta 8 host (servidores físicos y máquinas virtuales).

1.6.3 Estudio de la Metodología

La metodología que se definió para la detección de vulnerabilidades de los host más críticos (servidores físicos y máquinas virtuales) la comprenden tres fases, con las cuales se realizarán las pruebas de análisis de vulnerabilidades. [8]

La primera fase consiste en obtener tanta información como sea posible de los host que se encuentran sobre la red, para esto se realizan diferentes tipos de consultas a servidores DNS y técnicas que se basan en el análisis de los mensajes de enrutamiento. Se resalta que esta fase no busca obtener vulnerabilidad alguna, lo que se pretende con ella es obtener una lista lo más amplia posible sobre los host de la red objetivo. [9]

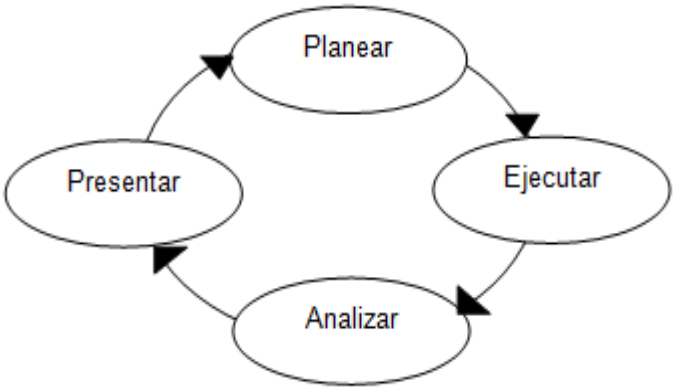
En la segunda fase llamada escaneo de puertos y enumeración de servicios, en

[8] UNIVERSIDAD DE CARTAGENA, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA. Metodología para la detección de Vulnerabilidades en Redes de Datos[2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos, el software que se utilizara para el escaneo son el Nessus y el Nmap que son primordiales para cumplir con los objetivos. [9]

Una vez obtenida la lista de los equipos de la red objetivo con presencia en internet y habiendo determinado cuáles de ellos juegan un rol crítico para la red, se procede a realizar la fase final de la metodología propuesta. La cual evaluará a los host críticos en busca de vulnerabilidades. Es en esta última fase se realiza la recolección y análisis de cada vulnerabilidad hallada en los host críticos que se hayan sido asignado. [9]

Figura 1. Proceso de la metodología aplicada



Fuente: Propiedad del Autor.

[9] MEDINA, Javier, Evaluación de vulnerabilidades TIC, [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=GSuZBgAAQBAJ&lpg=PA22&dq=pruebas%20de%20vulnerabilidades

2. MARCO DE REFERENCIA

2.1 MARCO TEORICO

2.2.1 Seguridad Informática[10]

La seguridad informática se enfoca en la protección de la integridad y privacidad de la información; se podría decir que en la seguridad informática se encarga de diseñar normas, procesamientos, métodos y técnicas, consiguiendo de esta forma un sistema de información seguro y confiable.

Para el establecimiento de un sistema de seguridad informática, necesario tener claro ciertos puntos:

- Cuáles son los elementos que componen el sistema.
- Cuáles son los peligros que afectan al sistema, ya sean provocados o accidentales.
- Cuáles son las medidas que se deberían acoger para lograr conocer y prevenir los riesgos potenciales.

Mediante la seguridad informática se debe asegurar que el acceso y la modificación a cierta información solo sea posible a las personas que estén autorizadas; un sistema se considera seguro si cumple con la integridad, confidencialidad y disponibilidad en la información:

- **Integridad:** Por medio de esta propiedad se garantiza que los datos no han sido alteradas y/o destruidos de modo no autorizados, es decir se garantiza la autenticidad de la información sin importar el momento.
- **Confidencialidad:** Se refiere al tributo que deben tener los datos y/o información, al encontrase únicamente al alcance de als personas y/o entidades autorizadas.
- **Disponibilidad:** Garantiza que la información se encuentra disponible para los usuarios siempre que lo necesiten, en caso contrario se provocan interrupciones de servicio y con ello problemas de calidad.

2.2.2 Auditoria Informática[10]

Es la revisión cuyo fin es detectar errores, fallas y fraudes con el propósito de establecer en realizar mejoras sobre las posibles incidencias que se pueda presentar en un sistema informático. Con la auditoria se puede definir, evaluar y obtener de manera objetiva las evidencias relacionada con informes sobre

[10] MOYANO ORJUELA, Luz. SUAREZ CÁRDENAS, Yasmin. Plan de Implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones. [2018] [en línea] [citado el 12 de diciembre, 2018] Disponible en internet: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

actividades o eventos a nivel informático.

La auditoría Informática permite ayudar a las organizaciones a comprobar la eficiencia del sistema, permitiendo verificar su funcionamiento se encuentra correctamente con los recursos adecuados, si cumple con la normativa y leyes que rigen en el sector, desde la protección de datos hasta aspectos ambientales.

2.2.3 Norma Técnica Colombiana NTC-ISO/IEC 27001[11]

Esta norma ha sido elaborada para brindar un modelo para el establece cimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización.

2.2.3.1 Enfoque basado en procesos NTC-ISO/IEC 27001[11]

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.

Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como proceso cualquier actividad que use recursos y cuya gestión permita la trasformación de entradas y salidas. El resultado de un proceso constituye directamente la entrada del proceso siguiente.

El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a sus usuarios a hacer énfasis en la importancia de:

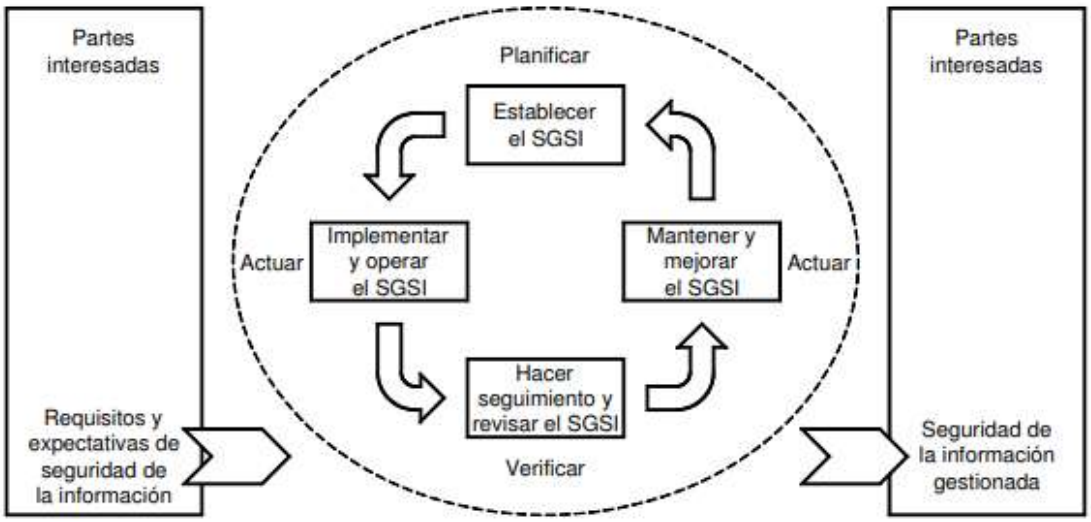
a) Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información.
b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de riesgos globales del negocio de la organización.
c) El seguimiento y revisión del desempeño y eficacia del SGSI.
d) La mejora continua basada en la medición de objetivos.

[11]ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001.] [citado el 08 de noviembre,2018] Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

2.2.3.2 Modelos de procesos (PHVA)[12]

La norma NTC-ISO/IEC 27001 adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI. La figura 2 ilustra como el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumple los requisitos y expectativas.

Figura 2. Modelo PHVA aplicado a los procesos SGSI



Fuente: ICONTEC, http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

La adopción del modelos PHVA también reflejara los principios establecidos en la directrices OCDE que controla la seguridad de sistemas y redes de información, esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

[12]ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001.] [citado el 08 de noviembre,2018] Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Tabla 1 PHVA aplicado a los procesos SGSI

Proceso	Descripción
Planificar (establecer el SGSI)	Establece la política, los objetivos, procesos y procedimiento de seguridad pertinente para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (Implementar y operar el SGSI)	Implementa y operar la política, los controles, procesos y procedimientos del SGSI
Verificar (Hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoria interna SGSI y la revsion por la dirección, para lograr a mejora continua.

Fuente: ICONTEC, http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

2.2.4 Riesgos[13]

El riesgo es una amenaza evaluada en cuanto a la gravedad de ocurrencia y a la gravedad potencial o consecuencia, permitiendo estimar las probabilidades de que una amenaza se materialice sobre los activos de una organización, causando efectos negativos o perdidos.

2.2.5 Amenazas[14]

Se define como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se

[13]Desenredados. Evaluación de amenaza, vulnerabilidad y el riesgo. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://nmap.org/

[14]Universidad Nacional de Lujan. Amenazas a la Seguridad de la Información. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

comprometa o no la seguridad de un sistema de información.

2.2.6 Vulnerabilidad[15].

Se define como un sistema (máquina o proceso) automatizado como aquel capaz de reaccionar de forma automática (sin la intervención humana) ante los cambios que se producen en el mismo, realizando las acciones adecuadas para cumplir la función para la cual ha sido diseñado. Las vulnerabilidades son las condiciones y características propias del sistema de una organización que la hacen susceptibles algún tipo de amenaza.

2.2.7 Nmap[16].

Nmap (Herramienta de exploración de redes y sondeo de seguridad / puertos) es una herramienta que se utiliza para explorar, administrar y auditar la seguridad de redes de hosts, detecta host online con sus respectivos puertos abiertos, servicios y aplicaciones corriendo sobre ellos y sus sistemas operativos, además identifica que firewall/filtros corren en una red. Generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios que se mantiene activos.

2.2.7.1 Características de Nmap[17]

La herramienta Nmap posee las siguientes características:

- Operación paralela de alta velocidad a través de sockets no bloqueantes y una gramática de definición de sonda, coincidencia diseñada para una implementación eficiente pero potente.
- Determina el nombre de la aplicación y el número de versión donde esté disponible, no solo el protocolo del servicio.
- Admite los protocolos TCP y UDP, así como los servicios de ASCII textual y binario empaquetado.
- Soporte multiplataforma, que incluye Linux, Windows, Mac OS X, FreeBSD / NetBSD / OpenBSD, Solaris y todas las demás plataformas en las que se sabe que funciona Nmap.

[15]INCIBE. Amenazas vs Vulnerabilidades. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[16]NMAP. Nmap. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nmap.org/man/es/index.html
[17]SECURITY HACKLABS. El sistema de detección de versiones de Nmap. [2018] [en línea] [citado el 12 de diciembre, 2018] Disponible en internet: https://securityhacklabs.net/articulo/el-sistema-de-deteccion-de-versiones-de-nmap

- Si se detecta SSL, Nmap se conecta usando OpenSSL (si está disponible) e intenta determinar qué servicio está escuchando detrás de esa capa de cifrado. Esto le permite descubrir servicios como HTTPS, POP3S, IMAPS, etc., así como proporcionar detalles de la versión.
- Si se descubre un servicio SunRPC, Nmap lanza su rectificadora RPC de fuerza bruta para encontrar el número de programa, el nombre y el número de versión.
- Se admite IPv6, incluidos TCP, UDP y SSL sobre TCP.
- Salida común de enumeración de plataforma (CPE) para la inter operación con otro software (parte de la información solo se incluye en la salida XML). Consulte la sección llamada 'Common Platform Enumeration (CPE)'.
- Contribuciones de la comunidad: si Nmap obtiene datos de un servicio que no reconoce, se imprime una huella digital de servicio junto con una URL de envío. Este sistema está modelado después del extremadamente exitoso proceso de envío de huellas dactilares de Nmap sistema de detención. Nuevas sondas y correcciones también pueden enviarse.
- Base de datos completa: Nmap reconoce más de mil firmas de servicios, que cubren más de 180 protocolos de servicio únicos de ACAP, AFP y AIM a XML-RPC, Zebedee y Zebra.

2.2.7.2 Ventajas y desventajas de Nmap[18]

Se Describen las ventajas y desventajas que posee la herramienta Nmap:

- **Ventajas de Namp:** Este programa incluso en sus versiones graficas es muy poderoso, y tiene opciones para realizar escaneos muy difícilmente detectables por las “victimas” o supervisores de red. Escanea cualquier rango de puertos que desees e incluso detecta el sistema operativo de la víctima, dando lugar a que el hacker identifique más claramente cómo puede acceder al equipo remoto.

- **Ventajas de Namp:** Entre más complejo sea el tipo de escaneo que se quiere realizar, el proceso de escaneo puede ser más tardado y tardar varios minutos antes de finalizar, la velocidad del escaneo depende básicamente de 3 factores, velocidad de la computadora de quien escanea(hacker), latencia en la red(si la red es lenta o rápida), y velocidad de respuesta y medidas de seguridad de la computadora escaneada(victima)

2.2.8 Kali Linux.

Es una herramienta capaz de pruebas de vulnerabilidades desarrollada por Offensive Security, considerada como una de las mejores herramientas de

[18] CODIGO PROGRAMACION. Herramientas básicas para hacking (Escaneo). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://codigoprogramacion.com/tag/nmap-hacking#.XBPM54tKiUk

auditorías de redes y seguridad informática en general. El sistema operativo Kali Linux ofrece los paquetes necesarios para el escaneo, análisis y explotación de vulnerabilidades incluyendo herramientas para análisis forenses.[19]

2.2.8.1 Característica del Sistema Operativo Kali Linux[20].

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, y hemos cambiado a Git para nuestro VCS.

- **Más de 300 herramientas de pruebas de penetración:** Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.
- **Gratis y siempre lo será:** Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.
- **Git – árbol de código abierto:** Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.
- **Obediente a FHS:** Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.
- **Amplio apoyo a dispositivos inalámbricos:** Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.
- **Kernel personalizado con parches de inyección:** Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.
- **Entorno de desarrollo seguro:** El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.

[19] KALI. Kali Linux. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.kali.org/

[20] INFORMÁTICA. Kali Linux: Una distribución Linux especializada. [2018] [en línea] [citado el 13 de diciembre, 2018] Disponible en internet: https://inforseguridad.wordpress.com/2016/11/09/kali-linux-que-es-para-que-se-utiliza-las-diez-aplicaciones-mas-importantes-que-integra/

- **Paquetes firmados con PGP y repos:** Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.
- **Multi-lenguaje:** Aunque las herramientas de penetración tienden a ser escritas en inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.
- **Totalmente personalizable:** Estamos completamente consiente de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan personalizar Kali Linux a su gusto, todo el camino hasta el núcleo.
- **Soporte ARMEL y ARMHF:** Dado a que los sistemas basados en ARM son cada vez más frecuentes y de bajo costo, sabíamos que el soporte de ARM de Kali tendrían que ser tan robusta como podríamos administrar, resultando en instalaciones que trabajan en sistemas de ARMEL y ARMHF. Kali Linux tiene repositorios ARM integrado con la línea principal de distribución de modo que las herramientas para ARM serán actualizada en relación con el resto de la distribución. Kali está disponible para los dispositivos ARM siguientes: rk3306 mk/ss808, Raspberry Pi, ODROID U2/X2, MK802/MK802 II, Samsung Chromebook.

2.2.8.2 Ventajas y desventajas de Kali Linux

Se Describen las ventajas y desventajas que posee del sistema operativo Kali Linux:

Hay 3 ventajas fundamentales de Linux que juntas le dan una gran consideración:

- Linux es muy robusto, estable y rápido: Ideal para servidores y aplicaciones distribuidas. A esto se añade que puede funcionar en máquinas de bajo recursos: Linux puede correr servicios en un x86 a 200 MHz con calidad.
- Linux es libre: Esto implica no sólo la gratuidad del software, sino también que Linux es modificable y que Linux tiene una gran cantidad de aplicaciones libres en Internet. Todo ello arropado por la inmensa documentación de Linux que puede encontrarse en la Red.
- Linux ya no está restringido a personas con grandes conocimientos de informática: Los desarrolladores de Linux han hecho un gran esfuerzo por dotar al sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente distribuciones Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows

Las desventajas de Linux pueden ser:

- Windows es incompatible con Linux: Este punto es difícil de explicar: no quiere decir que no podamos tener instalados ambos Sistemas (que es relativamente fácil de hacer)

  Uno de los problemas es que desde Windows no podremos escribir en particiones Linux o que desde Linux no podremos escribir (en sentido amplio) en particiones NTFS (Windows XP, 2000...) aunque esto último se está investigando

- En la mayoría de distribuciones Linux hay que conocer nuestro Hardware a la hora de instalar, sin embargo, distribuciones de Linux como Knoppix reconocen todo el sistema a lo Windows

2.2.9 Nessus[21]

Nessus es una extensión de archivo conocido como Network Security Scanner File Nessus que fue desarrollado por Tenable Network Security. Nessus es una aplicación de escaneo de vulnerabilidades de red.

Específicamente, el formato de archivo de datos guarda los resultados de un análisis de seguridad de red, así como las políticas utilizadas para la exploración realizada. Permite a los resultados de las exploraciones de empresa o red doméstica que se guarden y se importan para su revisión.

Los Archivos Nessus utilizan XML de formato que significa que es XML internamente introducido en Nessus 3.2, el formato de referencia todo el contexto de la exploración - la política real que se utiliza, el conjunto de plug-in usa, la lista de los objetivo para los datos de exploración, de importación y exportación de informes más fácil. Posee base de datos CVSS, factores de riesgo y más. Los archivos en formato Nessus se pueden abrir con el entorno único de Tenable Nessus en la Red de Seguridad en Microsoft Windows, Linux y plataformas Mac OS.

2.2.9.1 Características de Nessus[22]

Las características de Meses son variadas, ya que es un sistema de respuesta rápida que nos permite realizar exploraciones y análisis ad-hoc, capaz de auditar y analizar tanto los sistemas de red como los rastreos de archivos se seguridad y se adapta a diferentes plataformas y sistemas operativos, se describen las características importantes de Nessus:

[21] REVIVERSOFT. Nessus extensión del archivo. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.reviversoft.com/es/file-extensions/nessus

[22] EMPRESA Y ECONOMIA. Nessus, seguridad a la alta velocidad. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: http://empresayeconomia.republica.com/aplicaciones-para-empresas/nessus-seguridad-a-alta-velocidad.html

- Nessus es un escáner de vulnerabilidades que funciona mediante un proceso de alta velocidad.
- Encuentra los datos sensibles y trabaja con la auditoria de configuraciones y el perfil activo.
- Funciona tanto en sistemas operativos de Windows como en la gran parte de las plataformas de Unix.
- Realiza análisis de credenciales y aplicaciones que posean alto grado de seguridad.

2.2 MARCO CONCEPTUAL

" Pfleeger y Ciszek (2008), exponen una metodología compuesto de cuatro pasos que pretende ayudar a las organizaciones a evaluar los activos relevantes a ser protegidos, estableciendo los potenciales atacantes y los posibles métodos para disminuir el riesgo, sin embargo, no se precisan técnicas para evaluación de la seguridad de dichos activos" [23]

"podemos mencionar que en el campo de las aplicaciones Web sobresalen NeXpose (también útil para plataformas de escritorio), acunetix, w3af, entre otros. Algunos de estos proyectos han sido examinados en trabajos de investigación (Bau et al., 2010) donde se evaluaron ocho diferentes escáneres de vulnerabilidades de aplicaciones web, con el fin de determinar su efectividad en la detección de éstas. Además, otro trabajo (Shi et al., 2010) realizó la evaluación de diferentes herramientas de seguridad, a la vez que se compararon las habilidades de las mismas"[23]

“Pese a los trabajos que han sido realizados el problema que surge de la presencia de vulnerabilidades en redes de datos, sigue causando grandes pérdidas a organizaciones e individuos en la actualidad, por esto se han desarrollado diferentes metodologías para la detección de dichas vulnerabilidades (Watanabe et al., 2010)"[23]

2.2.1 Simulación de Intrusión (Test de Penetración) [24]

[23] FRANCO, David A. PEREA, jorge L. PUELLO, Plinio, Metodología para la detección de vulnerabilidades en redes de datos. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: http://bibliotecavirtual.unad.edu.co:2139/eds/pdfviewer/pdfviewer?vid=1&sid=8cd37457-4010-4308-a0ad-b3b98f16c321%40pdc-v-sessmgr03

[24] GUTIERREZ DE MORAL, Leonardo. Curso de ciberseguridad y hacking ético 2013, pág. 66. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=sua0BAAAQBAJ&lpg=PA66&dq=metodologia%20pentest&pg=PA67#v=onepage&q=metodologia%20pentest&f=false

"El PenTest es un ataque avanzado y bien estructurado hacia la infraestructura de información, dirigido hacia la evaluación de seguridad y detección temprana de fallas de seguridad. A continuación se describe algunos servicios que ofrece la simulación de intrusión:

Detectar vulnerabilidades que pueden ser explotadas por crackers para interrumpir el sistema.

- Analizar y priorizar las fallas de seguridad dependiendo el impacto que tendría sobre la información y la empresa en sí misma.
- proveer soluciones para reducir la probabilidad de una intrusión.
- estas simulaciones tiene por objetivo responder a las siguientes preguntas:
- ¿Qué puede saber un intruso de mi organización?
- ¿Qué puede hacer el intruso con esa información?
- ¿Cómo puedo detectar un ataque?

Se hace mención que un Hacker ético hace uso de las simulaciones de intrusión como herramienta para la detección de vulnerabilidades, por tanto dichas simulaciones deben estar basada a la metodología del hacking.

De acurdo con la metodología propuesta por The Penetration Testing Framenwork (PTF) del Information System Security Assessment Framework (ISSAF), un proceso completo de evaluación de seguridad de un sistema de información debe dividirse en las fases:

I. Planeación y preparación
II. Evaluación
III. Reporte, limpieza y destrucción de huellas.

Estas 3 fases definen el trabajo total de un Hacker ético dentro de una organización, siendo la fase de evaluación del proceso central de la metodología ya que es la intrusión o penetración de un sistema.

Para lograr una intrusión exitosa se requiere dividir el proceso de ataque en 5 fases, donde cada una tiene un objetivo específico para lograr la intrusión. A continuación se muestran las fases de un ataque:

1. Recopilación de Información y Reconocimiento: Es el proceso de obtención y validación de la conectividad con el objetivo mediante la monitorización de la red.

2. Escaneo y Enumeración: Se identifica y enumeran todos los servicios y aplicaciones vulnerables. Debe incluir un escaneo intensivo del objetivo a identificar:

- Puertos accesibles.
- Localización de Gateway.

- Detalles del Sistema Operativo.
- Host accesibles.

3. Acceso a la red y los sistemas (ataque puro): Es el proceso de obtención de acceso que generalmente puede ser mediante:

- **Abuso:** Hacer uso legítimo de un medio de acceso.
- **Subversión: Hacer** que un servicio o aplicación se comporte de una manera no prevista por los programadores para obtener un acceso.

4. Mantenimiento de acceso y escalamiento de privilegios: Se aprovecha el modo inicial de acceso para ganar privilegios adicionales en el objetivo. Generalmente es en esta fase cuando un atacante instala un canal de comunicación oculto para transferir información desde su objetivo, método conocido como Backdoor.

5. Borrado de huellas: Proceso de destrucción de datos, aplicaciones o código que pueda delatar o brindar información sobre la ubicación del atacante (generalmente la dirección IP). Se pretende evitar que tras un análisis forense, se descubra información comprometedora del atacante, es importante mencionar que un ataque más intrusivo tiene una mayor posibilidad de ser descubierto".[25]

2.3 ANTECEDENTES

En la organización caso de estudio, hace más de un año realizó escaneo de vulnerabilidades, con lo cual no se ha vuelto realizar análisis, ya que por necesidad se requiere evaluar la seguridad de los host más críticos (Servidores físicos y máquinas virtuales).

Se presenta algunos antecedentes de trabajos realizados de análisis de vulnerabilidades:

"**Título:** Metodología para la Detección de Vulnerabilidades en Redes de datos

Autores: David Franco, Jorge Perea, Plinio Puello

Resumen: El objetivo principal de este trabajo fue diseñar una metodología para la detección de vulnerabilidades en redes de datos. Para esto se desarrollaron diferentes fases llamadas reconocimiento**,** escaneo de puertos y enumeración de servicios, y escaneo de vulnerabilidades, cada una de las cuales

[25] GUTIERREZ DE MORAL, Leonardo. Curso de ciberseguridad y hacking ético 2013, pág. 66. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=sua0BAAAQBAJ&lpg=PA66&dq=metodologia%20pentest&pg=PA67#v=onepage&q=metodologia%20pentest&f=false

es soportada por herramientas de software. Los resultados de cada fase suministran datos necesarios para la ejecución de las siguientes etapas. Con el fin de validar la utilidad de la metodología propuesta se llevó a cabo su implementación en la red de datos de la Universidad de Cartagena en Colombia, encontrando diferentes tipos de vulnerabilidades. Finalmente apoyándose en los resultados obtenidos, se encontró que la metodología propuesta es de gran utilidad para detectar vulnerabilidades en redes de datos, lo que demuestra su importancia para el área de la seguridad informática."[26]

"Título: Metodología de Análisis de Vulnerabilidades para Empresas de Mediana y Pequeña Escala

Autores: Daniel Santiago Garzón, Juan Carlos Ratkovich Gomes, Alejandro Vergara torres

Resumen: El siguiente artículo da una perspectiva global de un proceso de investigación sobre seguridad informática, específicamente en el aseguramiento de los recursos de la empresa, tomando como base cinco pilares fundamentales de la seguridad informática, integridad, confidencialidad, disponibilidad, adaptabilidad y no repudio, enfocándose en empresas de mediana y pequeña escala. El resultado de esta investigación fue una metodología la cual da a conocer una serie de pasos, que abarcan diferentes temas como son la planeación, políticas de seguridad, aseguramiento de los recursos de la compañía entre otros. Cada uno de estos temas ayuda al mejoramiento de la seguridad de la información, haciendo que un sistema permanezca cubierto y preparado ante eventualidades que puedan interrumpir el desarrollo normal de las actividades de la organización."[27]

2.4 MARCO LEGAL

2.4.1 Ley 1266 de 2008[28]

"Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la

[26] FRANCO, David A. PEREA, Jorge L. PUELLO, Plinio, Metodología para la detección de vulnerabilidades en redes de datos. [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: http://bibliotecavirtual.unad.edu.co:2139/eds/pdfviewer/pdfviewer?vid=1&sid=8cd37457-4010-4308-a0ad-b3b98f16c321%40pdc-v-sessmgr03

[27] UNIVERSIDAD DE CARTAGENA, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA. Metodología para la detección de Vulnerabilidades en Redes de Datos [2018] [en línea] [citado el 08 de noviembre,2018] Disponible en internet: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

[28] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

2.4.2 Ley 1581 de 2012[29]

"Por medio de esta se busca proteger la información de las personas que esté en poder de empresas públicas o entidades privadas, las cuales tienen la responsabilidad de adaptar sus procesos con el fin de realizar un manejo adecuado de sus bases de datos."

2.4.3 Ley 1341 de 2009[30]

"Por la cual se definen principios y conceptos sobre la sociedad de la información y las tecnologías de la información y las telecomunicaciones TIC".

2.4.4 Ley 1273 de 2009[31]

"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".

[29] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (Octubre 17 de 2012). Diario Oficial 48.587 de octubre 17 de 2012. p. 1-16.
[30] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341. Bogotá. (Julio 30 de 2009). Diario Oficial 47.426 de julio 30 de 2009. p. 1-10.
[31] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (Enero 5 de 2009). Diario Oficial 47.223 de enero 5 de 2008. p. 1-3.

3 RECOLECCIÓN DE INFORMACIÓN DE LOS HOST MÁS CRÍTICOS DE LA ORGANIZACIÓN CASO DE ESTUDIO.

Se listan los host críticos obtenidos mediante el inventario de infraestructura y validados por los administradores de servidores y el directorio activo que se muestra en la tabla 2. Listado de Host críticos de la organización caso estudio, los activos son asignados para realizar el escaneo y análisis vulnerabilidades en la organización caso de estudio.

Tabla 2. Listado de Host Críticos de la Organización Caso estudio

LISTADO DE HOST CRITICOS DE LA ORGANIZACIÓN CASO ESTUDIO				
#	**NOMBRE DE HOST**	**HOST**	**DESCRIPCION**	**RESPONSABLE**
1	ob01tc01	172.16.x.x	Base de datos aplicaciones Site	Infraestructura
2	cb02tc01	172.16.x.x	Base de datos Reports	Infraestructura
3	pt41tc01	172.16.x.x	Aplicaciones Kactus	Infraestructura
4	zw03tc01	172.16.x.x	Producción base de datos Kactus.	Infraestructura
5	zy03tc01	172.16.x.x	Morfeus	Infraestructura
6	ba03tc01	172.16.x.x	Servidor de backup SICA	Infraestructura
7	ba03tc01	172.16.x.x	Servidor de backup SICA	Infraestructura
8	rs01tc01	172.16.x.x	Repositorio base de datos RST	Infraestructura
9	oa03tc01	172.16.x.x	Servidor DA	Infraestructura
10	zr0ttc01	172.16.x.x	Servidor de aplicaciones SICA	Infraestructura
11	sz02tc01	172.16.x.x	Repositorio Base de datos SICA	Infraestructura
12	zz01tc01	172.16.x.x	Producción Jones	Infraestructura
13	ba03tc01	172.x.x	Servidor backup publiquemos	Infraestructura
14	oa11tc01	172.16.x.x	Publiquemos 1	Infraestructura
15	oa02tc01	172.16.x.x	Publiquemos 2	Infraestructura

Fuente: Propiedad del Autor

Mediante la ejecución de análisis de vulnerabilidades en los host es efectuado con el fin de incrementar la seguridad de aquellas brechas de vulnerabilidades que serán identificadas, con tal fin después sean mitigados por el grupo área del tecnología y cómputo de la organización caso de estudio de la organización caso de estudio.

A continuación se describe los servicios asignados, evaluados y que serán analizados para cumplir con el respectivo escaneo de vulnerabilidades mostradas en la Tabla 3. Host críticos de la organización caso de estudio:

Tabla 3. Host Críticos de la Organización caso de estudio

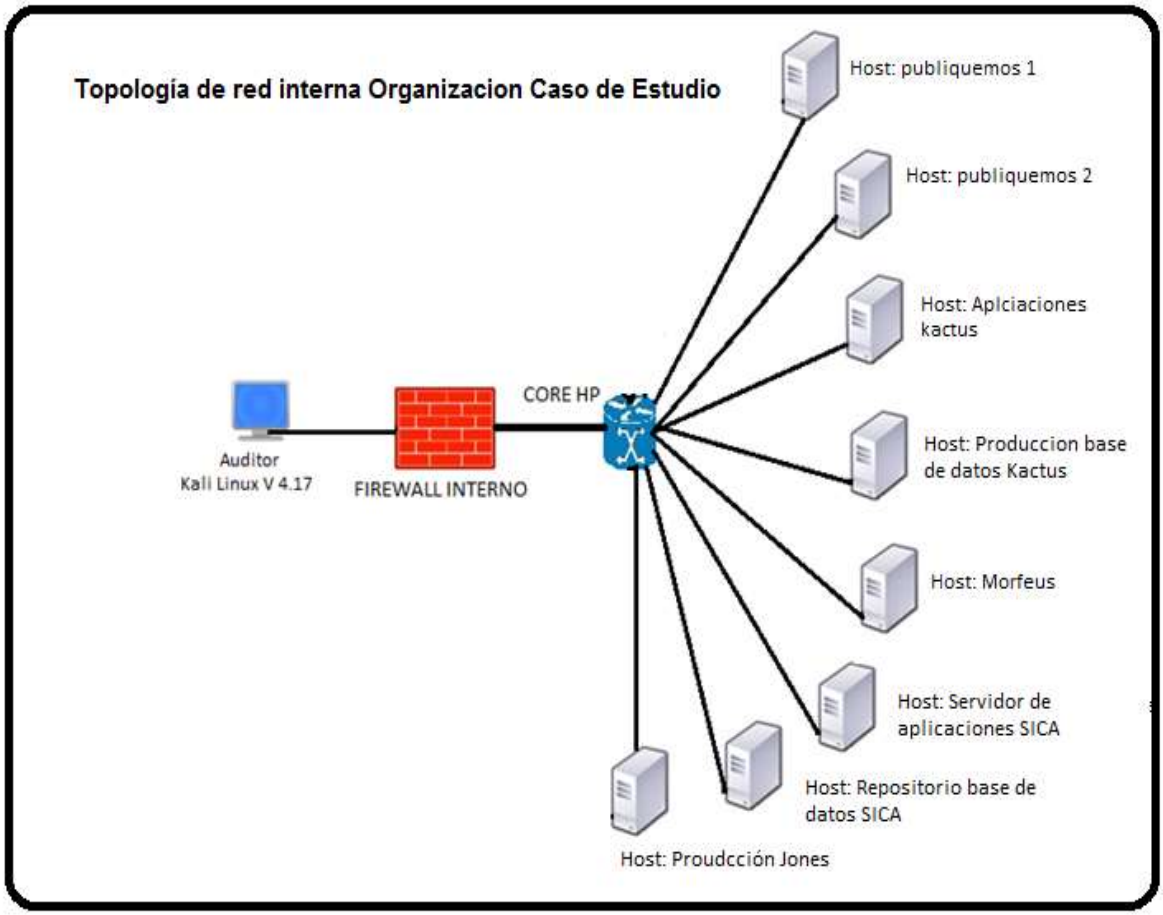
HOST CRITICOS DE LA ORGANIZACIÓN CASO ESTUDIO			
NOMBRE DE HOST	**HOST**	**DESCRIPCION**	**RESPONSABLE**
oa11tc01	172.16.x.x	Publiquemos 1	Infraestructura
oa02tc01	172.16.x.x	Publiquemos 2	Infraestructura
pt41tc01	172.16.x.x	Aplicaciones Kactus	Infraestructura
zw03tc01	172.16.x.x	Producción base de datos Kactus.	Infraestructura
zy03tc01	172.16.x.x	Morfeus	Infraestructura
zr03tc01	172.16.x.x	Servidor de aplicaciones SICA	Infraestructura
sz02tc01	172.16.x.x	Repositorio Base de datos SICA	Infraestructura
zz01tc01	172.16.x.x	Producción Jones	Infraestructura

Fuente: Propiedad del Autor

3.1 TOPOLOGÍA DE RED DE LOS HOST MAS CRITICOS

En el contexto de escaneo de vulnerabilidades, se ejecuta el procedimiento de escaneo y analisis en la misma la red interna de la organización, se resalta que no es necesario contar con permisos especiales en el firewall ya que el auditor posee privilegios sobre el sistema y la red la vlan se encuentra dentro de la misma red de gestion y administacion de los host criticos, ademas se tiene encuenta que los host son enlances segmentados por vlans en la misma red como se muestra en la figura 3. Topología de red interna de la organización caso de Estudio.

Figura 3. Topología de red interna de la Organización Caso de Estudio



Fuente: Propiedad del Autor

En la organización caso de estudio cuenta con una red que lo conforma un sistema de seguridad perimetral, incluyendo un firewall que divide la red interna con la red externa, para el proceso de escaneo se validó que la maquina auditor Kali Linux estuviera sobre la misma Vlan para enlazar conectividad con los host críticos, asimismo aplicar los respectivos métodos de “Pen Test”.

4. VERFICACIÓN DE VULNERABILIDADES A TRAVES DE PRUEBAS DE PENETRACION EN LA ORGANIZACIÓN CASO ESTUDIO.

4.1 PRUEBAS DE PENETRACION NESSUS.

Para los respectivo escaneos de vulnerabilidades de los host críticos se realiza el respectivo alistamiento de las herramientas Nessus, una vez realizado el proceso de instalación y configuración se procede a realizar los procedimientos requeridos.

4.1.1 Instalación de Nessus.

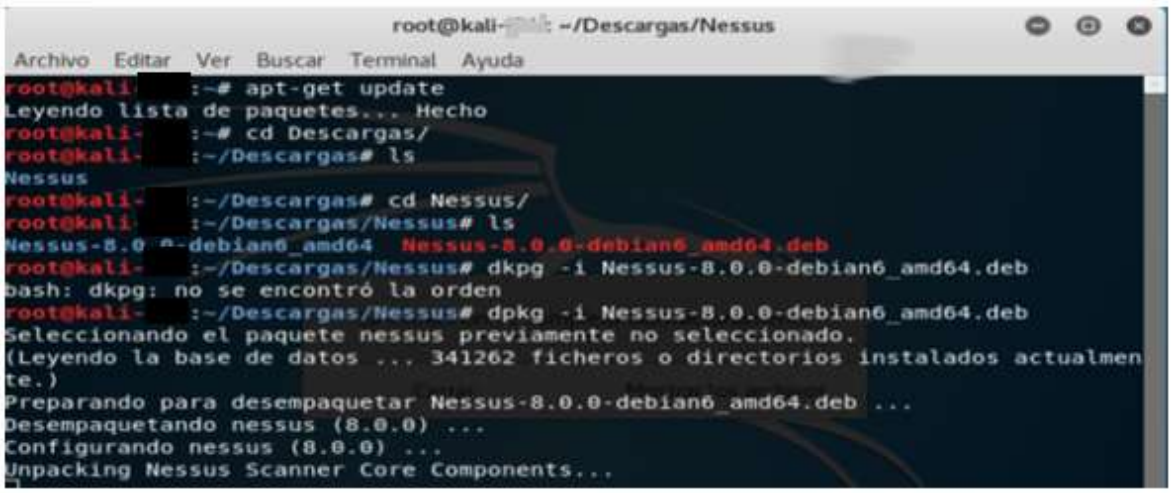
Para el funcionamiento de la herramienta Nessus se utiliza un equipo cumpliendo con los requisitos recomendados por Nessus con las siguientes características:

- Equipo: Computador HP 205 dos en uno
- Procesador: Doble núcleo AMD E1-2500 (1.48 Ghz, 1MB, 2 de cache. 2 núcleos)
- Tarjeta de gráficos integrada: AMD Radeom HD 8240
- Memoria RAM: 8GB (1x8 GB) DDR3
- Sistema Operativo: Sistema Operativo Kali Linux (64 Bits) instalado y dedicado

Para el correcto funcionamiento home de Nessus se realiza la actualización e instalación de paquetes en Kali Linux en la consola mediante los comandos como se muestra en la Figura 4. Actualización de paquetes:

- Actualización de paquetes:
  apt- get update
- Instalación de paquetes:
  apt- get upgrade

Figura 4. Actualización de paquetes

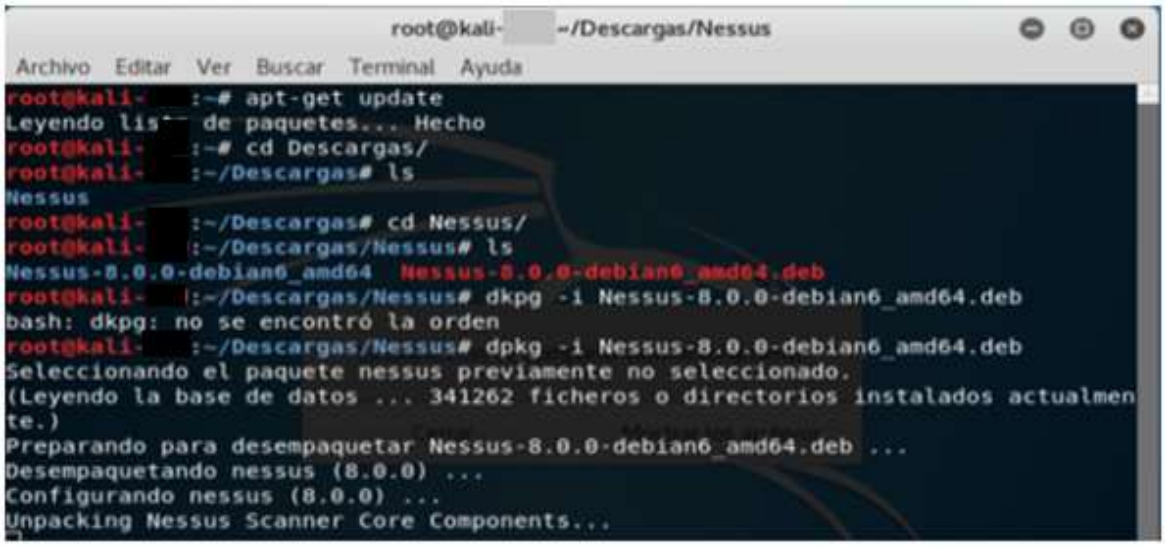


Fuente: Propiedad del Autor.

Debidamente actualizado los paquetes necesarios, seguimos con el proceso de instalación, en la página https://www.tenable.com/downloads/nessus a descargamos el “Nessus 8.0.0-debian6_amd64.deb”, descomprimido el archivo e ingresando a la ruta donde se encuentra alojado el software, instalamos la herramienta con el comando como se observa en la Figura 5. Instalación de Nessus:

Dpkg -i Nessus 8.0.0-debian6_amd64.deb

Figura 5. Instalación de Nessus.

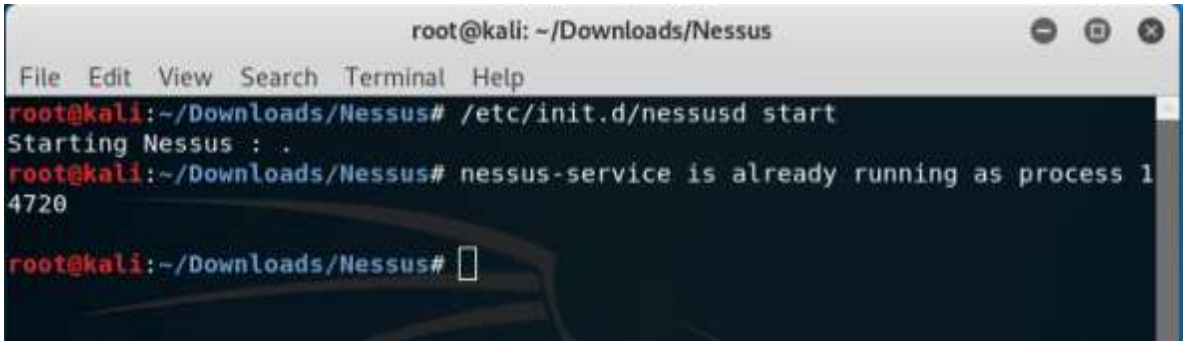


Fuente: Propiedad del Autor.

Instalado los paquetes de Nessus damos inicio la herramienta como se muestra en la Figura 6. Inicios de Nessus mediante el comando:

/etc/init.d y ejecutar ./nessusd start

Figura 6. Inicio de Nessus



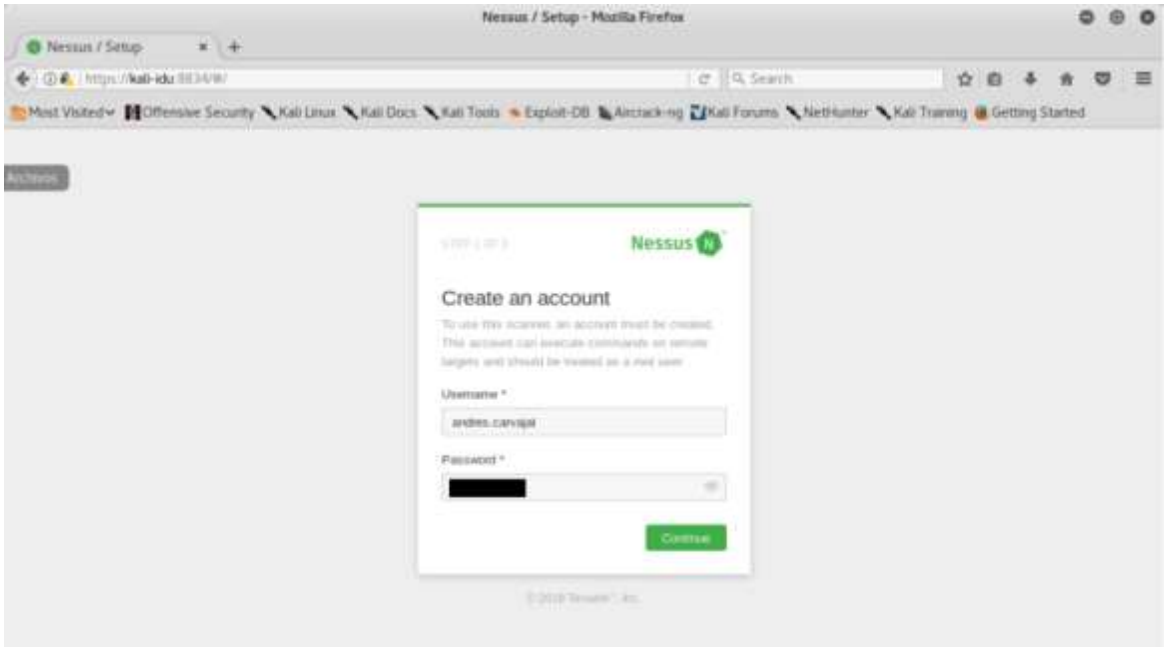
Fuente: Propiedad del Autor

4.1.2 Configuración de Nessus.

Para utilizar la herramienta es necesario registrase en la página https://www.tenable.com/ ya que es un requisito para poder utilizar los recursos ofrecidos por Nessus.

Ahora si procedemos a autenticarnos en la página https://kali:8834/ de Nessus como se puede apreciar en la Figura 7. Acceso al entorno Nessus:

Figura 7. Acceso al entorno de Nessus.

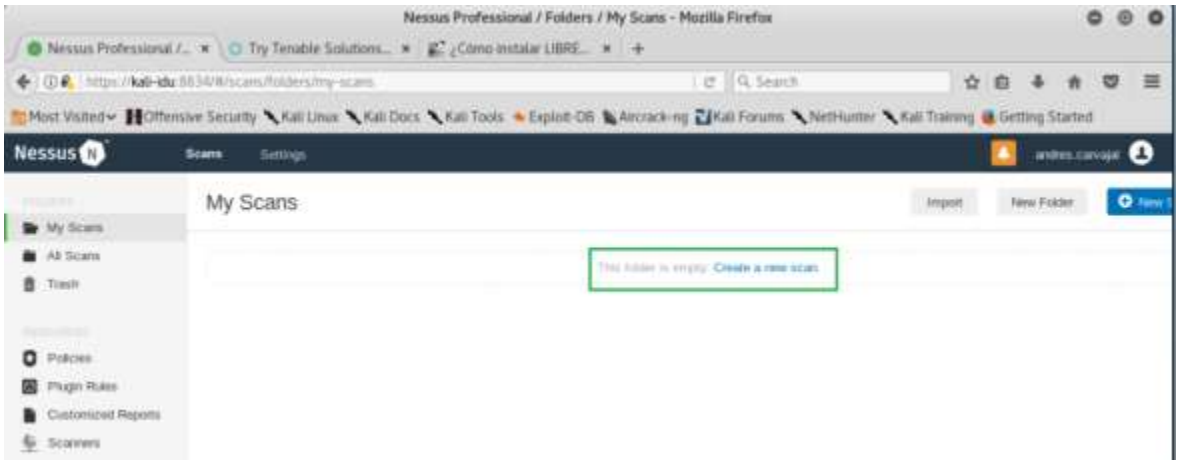


Fuente: Propiedad del Autor.

Una vez registrados en la página de Nessus, envía el código de activación para terminar con el proceso.

En el siguiente paso se realizara la creación de escaneos por cada host crítico de la organización caso de estudio como muestra en la Figura 8. Creación de nuevo escaneo.

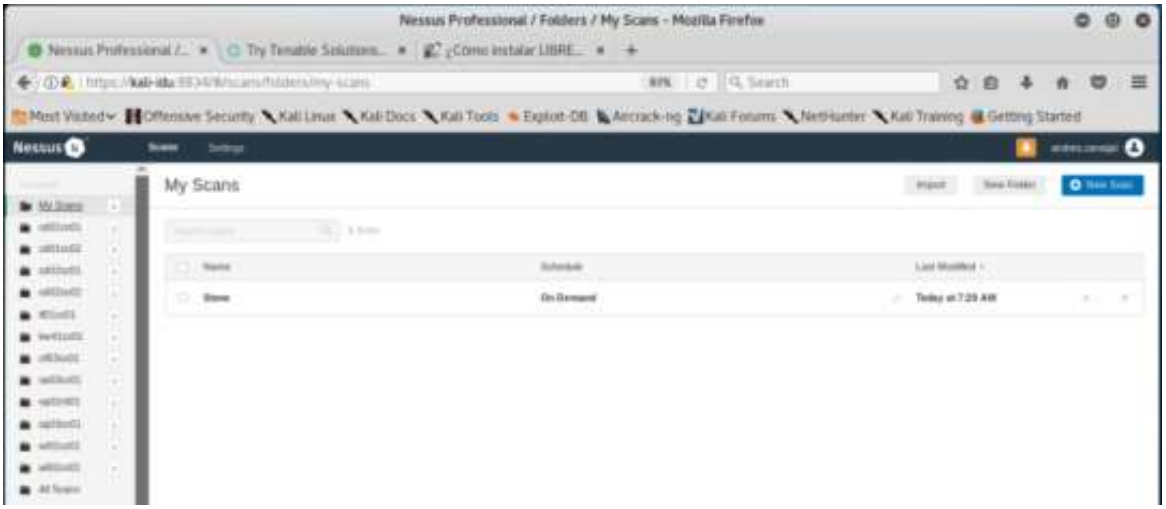
Figura 8. Creación de nuevo Escaneo



Fuente: Propiedad del Autor

Una vez listado cada Host con su respectiva configuración de nombre de host, Dirección IP y la información necesaria, empieza el proceso de Escaneo de vulnerabilidades de cada host asignado en la tabla 3. Host Críticos de la organización caso estudio, como se muestra en la figura 9. Lista de cada host configurado para escaneo de vulnerabilidades.

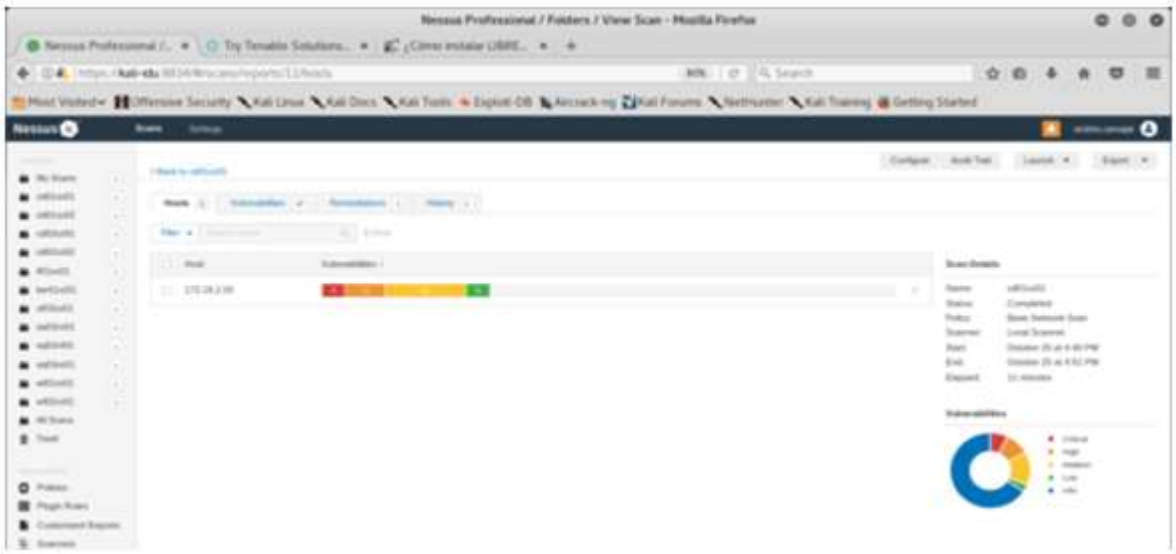
Figura 9. Lista de cada host configurado para escaneo de vulnerabilidades



Fuente: Propiedad del Autor.

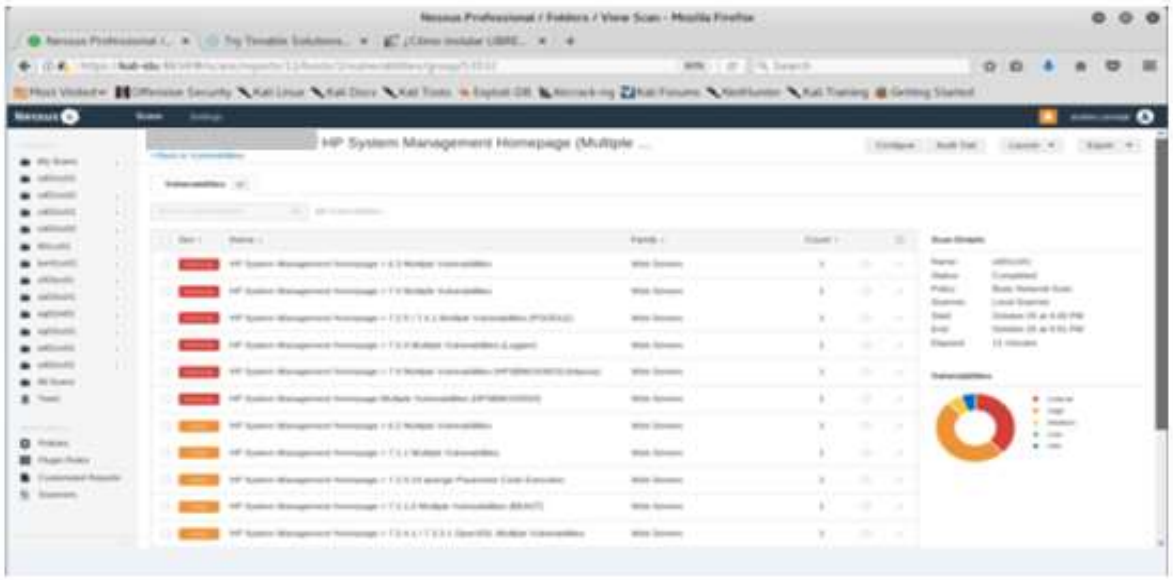
Terminado el proceso de Escaneo, nos muestra la información correspondiente: host, vulnerabilidades, remediaciones e historial como se muestra en la figura 10. Entorno información del Host Escaneado.

Figura 10. Entorno de Información del Host Escaneado.



Fuente: Propiedad del Autor.

Figura 11. Vulnerabilidades del Host Escaneado.



Fuente: Propiedad del Autor.

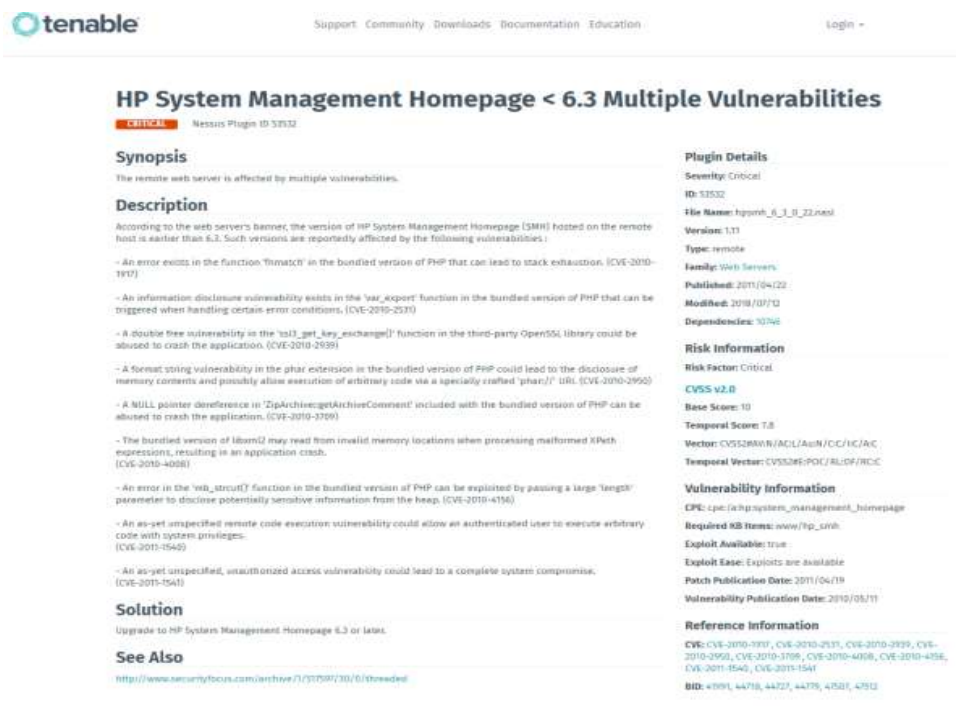
La herramienta ¨Nessus posee la opción de consultar con el enlace de la CVE, si le damos click, nos redirecciona a la página NVD (National Vulerability Database) o la página Tenable donde nos informa cada Vulnerabilidad y nos muestra información detallada de la vulnerabilidad detectada en el escaneo realizado mostrado en la figura 12. Referencia de vulnerabilidades CVE.

Figura 12. Referencia de vulnerabilidades CVE.

Fuente: Propiedad del Autor.

Finalmente, ingresando a la referencia de la vulnerabilidad se observara la información pertinente a cada severidad hallada son el host como se muestra en la Figura 13. Informes de vulnerabilidades.

Figura 13. Informe de vulnerabilidades CVE.



Fuente: Propiedad del Autor.

4.1.3 Vulnerabilidades halladas con Nessus.

Realizado la respectiva configuración e instalación procedemos a realizar el escaneo con la herramienta Nessus por cada uno de los host listados en la Tabla 3. Host Críticos de la Organización caso de estudio.

4.1.3.1 Escaneo con Nessus publiquemos 1 host: oa11tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host oa11tc01 mediante la herramienta de Nessus:

Figura 14. Información del Host oa11tc01.

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Crítica del Host oa11tc01: 1.**

El host oa11tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 4. Severidad critica del host oa11tc01

Tabla 4. Severidad Crítica del host oa11tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Alta del Host oa11tc11: 1.**

El host oa01tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 5. Severidad alta del host oa11tc01

Tabla 5. Severidad Alta del host oa11tc01.

HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Media del Host oa11tc01: 6.**

El host oa01tc01 presenta seis vulnerabilidades que requieren atención de tipo estándar, como se muestra en la tabla 6. Severidad media del host oa11tc01.

Tabla 6. Severidad Media del host oa11tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor.

4.1.3.2 Escaneo con Nessus publiquemos 2 host: oa02tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host oa02tc01 mediante la herramienta de Nessus:

Figura 15. Información del Host oa02tc01.

Host Information	
OS:	Microsoft Windows 7, Microsoft Windows Server 2008 R2

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Crítica del Host oa02tc01: 1**

El host oa02tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 7. Severidad critica del host oa02tc01.

Tabla 7. Severidad Crítica del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Alta del Host oa02tc01: 1**.

El host oa02tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 8. Severidad alta del host oa02tc01.

Tabla 8. Severidad Alta del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Media del Host oa02tc01: 6.**

El host oa02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 9. Severidad media del host oa02tc01

Tabla 9. Severidad Crítica del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor.

4.1.3.3 Escaneo con Nessus aplicaciones kactus host: pt41tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host pt41tc01 mediante la herramienta de Nessus:

Figura 16. Información del Host pt41tc01.

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Crítica del Host pt41tc01: 2**

El host pt41tc01 presenta dos vulnerabilidades de alto grado de impacto, como se

muestra en la tabla 10. Severidad critica del host pt41tc01.

Tabla 10. Severidad Crítica del host pt41tc01.

SEVERITY	CVSS	PLUGIN	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)

Fuente: Propiedad del Autor

- **Vulnerabilidad de Severidad Crítica del Host pt41tc01: 1.**

El host pt41tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 11. Severidad alta del host pt41tc01.

Tabla 11. Severidad Alta del host pt41tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Media del Host pt41tc01: 9.**

El host pt41tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 12. Severidad media del host pt41tc01.

Tabla 12. Severidad Media del host pt41tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

4.1.3.4 Escaneo con Nessus producción base de datos kactus host: zw03tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host zw03tc01 mediante la herramienta de Nessus:

Figura 17. Información del Host zw03tc01.

Fuente: Propiedad del Autor

- **Vulnerabilidad Severidad Crítica del Host zw03tc01: 4.**

El host zw03tc01 presenta cuatro vulnerabilidades de alto grado de impacto, como se muestra en la tabla 13. Severidad critica del host zw03tc01.

Tabla 13. Severidad Crítica del host zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	94654	HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy)
CRITICAL	10.0	91222	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)
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)

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Alta del Host zw03tc01: 1.**

El host zw03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 14. Severidad Alta del host zw03tc01.

Tabla 14. Severidad Alta del host zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.8	103530	HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753)

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Media del Host zw03tc01: 10**

El host zw03tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 15. Severidad media del host zw03tc01

Tabla 15. Severidad Media del host: zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required

Fuente: Propiedad del Autor.

4.1.3.5 Escaneo con Nessus Morfeus host: zy03tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host zy03tc01 mediante la herramienta de Nessus:

Figura 18. Información del Host en zy03tc01.

Host Information

OS:	Linux Kernel 2.6 on CentOS Linux release 6

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Crítica del Host zy03tc01: 0.**

En el en zy03tc01 no se encontró ninguna severidad crítica que pueda comprometer el host.

- **Vulnerabilidad de Severidad Alta del Host zy03tc01: 1.**

El host zy03tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 16. Severidad Alta del host zy03tc01.
Tabla 16. Severidad Alta del host en zy03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Media del Host zy03tc01: 7.**

El host zy03tc01 presenta siete vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 17. Severidad media del host zy03tc01
Tabla 17. Severidad Media del host en zy03tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

4.1.3.6 Servidor de aplicaciones sica host: zr03tc01 ip: 172.16.x.x.

Se realiza el escaneo de vulnerabilidades del host zr03tc01 mediante la herramienta de Nessus:

Figura 19. Información del Host zr03tc01.

Host Information

OS:	Microsoft Windows Server 2008 R2 Standard

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Crítica del Host zr03tc01: 3.**

El host zr03tc01 presenta tres vulnerabilidades de alto grado de impacto, como se muestra en la tabla 18. Severidad critica del host zr03tc01.

Tabla 18. Severidad Crítica del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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	108797	Unsupported Windows OS

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Alta del Host zr03tc01: 1.**

El host zr03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 19. Severidad Alta del host zr03tc01.

Tabla 19. Severidad Alta del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Media del Host zr03tc01: 9.**

El host zr03tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 20. Severidad media del host zr03tc01.

Tabla 20. Severidad Media del host zr03tc01

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low

Fuente: Propiedad del Autor.

4.1.3.7 Escaneo con Nessus repositorio base de datos sica host: sz02tc01 ip: 172.16.x.x

Figura 20. Información del Host sz02tc01.

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Crítica del Host sz02tc01: 2.**

El host sz02tc01 presenta dos vulnerabilidades de alto grado de impacto, como se muestra en la tabla 21. Severidad critica del host sz02tc01.

Tabla 21. Severidad Crítica del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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)

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Alta del Host sz02tc01: 2.**

El host sz02tc01 presenta dos vulnerabilidades que requiere atención de inmediata, como se muestra en la tabla 20. Severidad Alta del host sz02tc01

Tabla 22. Severidad Alta del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Media del Host sz02tc01: 11.**

El host sz02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 23. Severidad media del host sz02tc01

Tabla 23. Severidad Media del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Fuente: Propiedad del Autor.

4.1.3.8 Escaneo con Nessus producción jones host: zz01tc01 ip: 172.16.x.x

Se realiza el escaneo de vulnerabilidades del host zz01tc01 mediante la herramienta de Nessus:

Figura 21. Información del Host zz01tc01.

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Crítica del Host zz01tc01: 1.**

El host zz01tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 24. Severidad critica del host zz01tc01.

Tabla 24. Severidad Crítica del host zz01tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)

Fuente: Propiedad del Autor.

- **Vulnerabilidad de Severidad Alta del Host zz01tc01: 0.**

En el Host zz01tc01 no se encontró ninguna severidad alta que pueda comprometer el host.

- **Vulnerabilidad de Severidad Media del Host zz01tc01: 9.**

El host zz01tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 25. Severidad media del host zz01tc01.

Tabla 25. Severidad Media del host zz01tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Fuente: Propiedad del Autor.

4.2 PRUEBAS DE PENETRACION CON NMAP

Para los respectivo escaneos de puertos de servicios de los host críticos se realiza el respectivo alistamiento de las herramientas Nmap, una vez realizado el proceso de instalación y configuración se procede a realizar los procedimientos requeridos.

4.2.1 Instalación de Nmap.

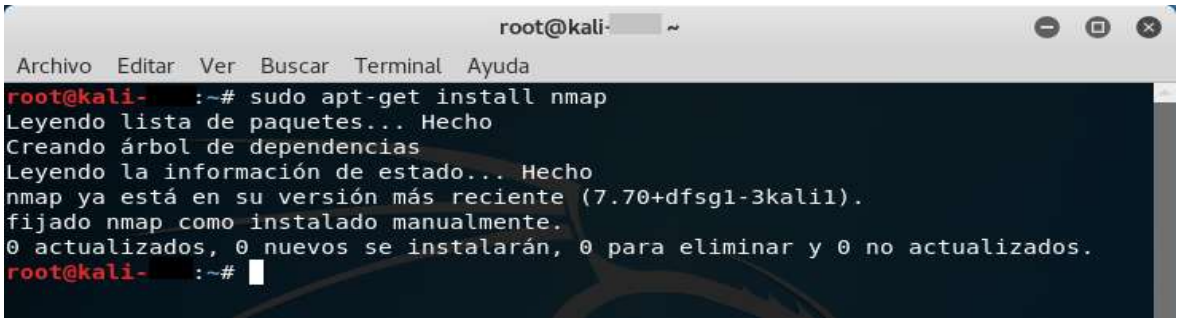
Para el funcionamiento de la herramienta Nmap se utiliza un equipo cumpliendo con los requisitos y las siguientes características:

- Equipo: Computador HP 205 dos en uno
- Procesador: Doble núcleo AMD E1-2500 (1.48 Ghz, 1MB, 2 de cache. 2 núcleos)
- Tarjeta de gráficos integrada: AMD Radeom HD 8240
- Memoria RAM: 8GB (1x8 GB) DDR3
- Sistema Operativo: Sistema Operativo Kali Linux (64 Bits) instalado y dedicado

Para la instalación de Nmap se realiza en kali Linux mediante los comandos como se muestra en la Figura 22. Instalación de Nmap en Kali Linux:

sudo apt- get install nmap

Figura 22 Instalación de Nmap en Kali Linux.



Fuente: Propiedad del Autor.

4.2.2 Configuración de Nmap

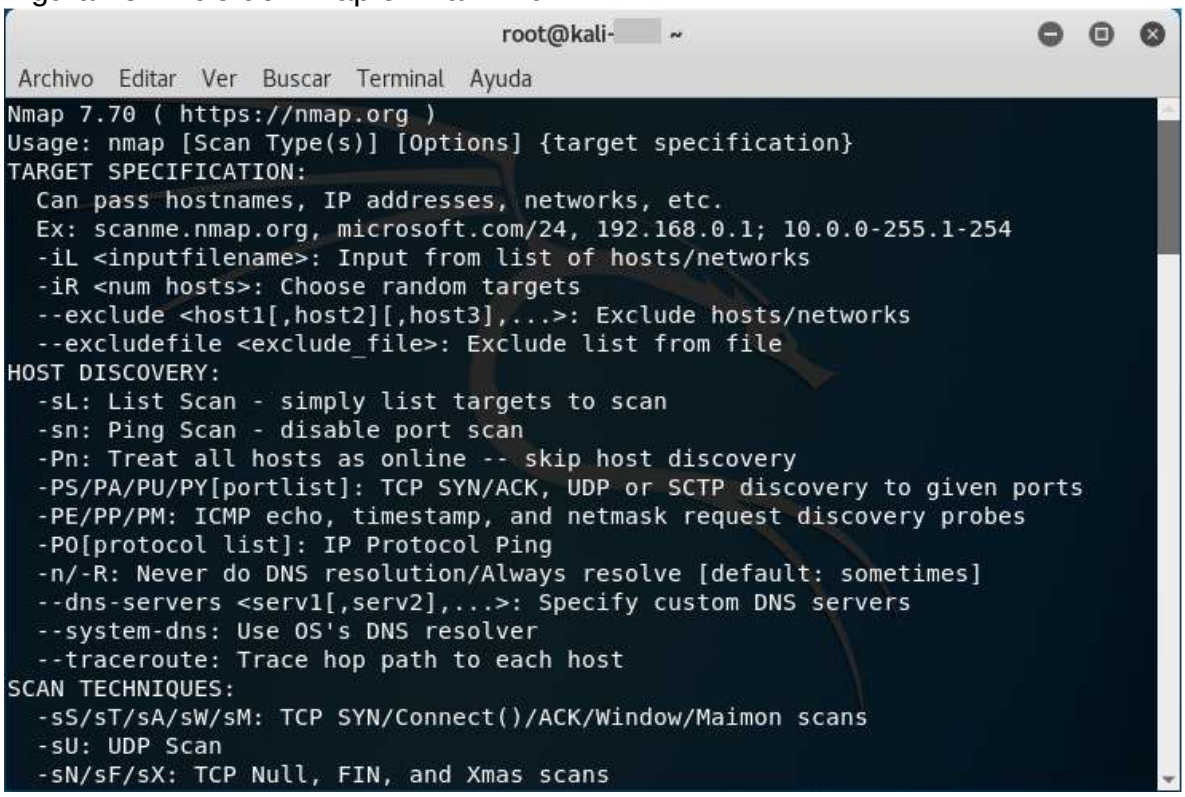
Para el proceso de configuración se realiza la actualización de paquetes en kali Linux en la consola mediante los comandos:

- Actualización de paquetes:
  sudo apt- get update

- Instalación de paquetes:
  apt- get upgrade

Finalizando la configuración, se procede a iniciar Nmap como se observa en la figura 23.

Figura 23. Inicio de Nmap en Kali Linux



4.2.3 Vulnerabilidades halladas con Nmap

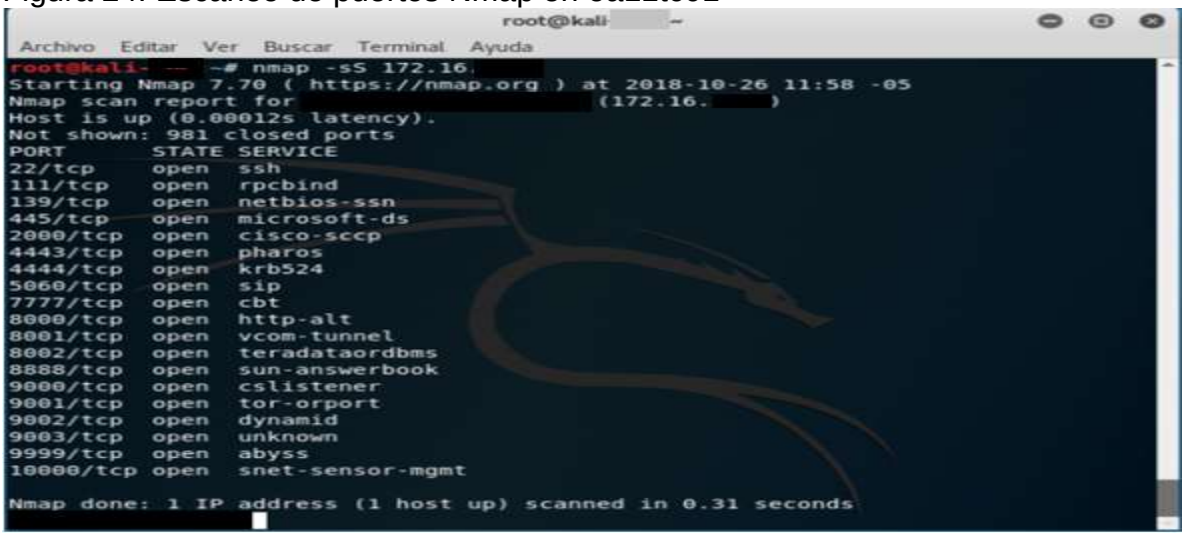
El consecuente procedimiento se realizara el escaneo de puertos de servicios aplicado a los host críticos mediante la herramienta Nmap que se encargará en muestrear los servicios abiertos y disponibles, para conocer el estado real de los host críticos.

Los servicios que se encuentra filtrados, son generalmente puertos TCP y/o UPD realizados mediante el método de escaneos relacionados con la base de datos nmap-services-probes para consultar distintos servicios que posee cada host,

4.2.3.1 Escaneo de puertos en publiquemos 1 host: oa11tc02 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 24. Escaneo de puertos Nmap en oa11tc01

Figura 24. Escaneo de puertos Nmap en oa11tc01

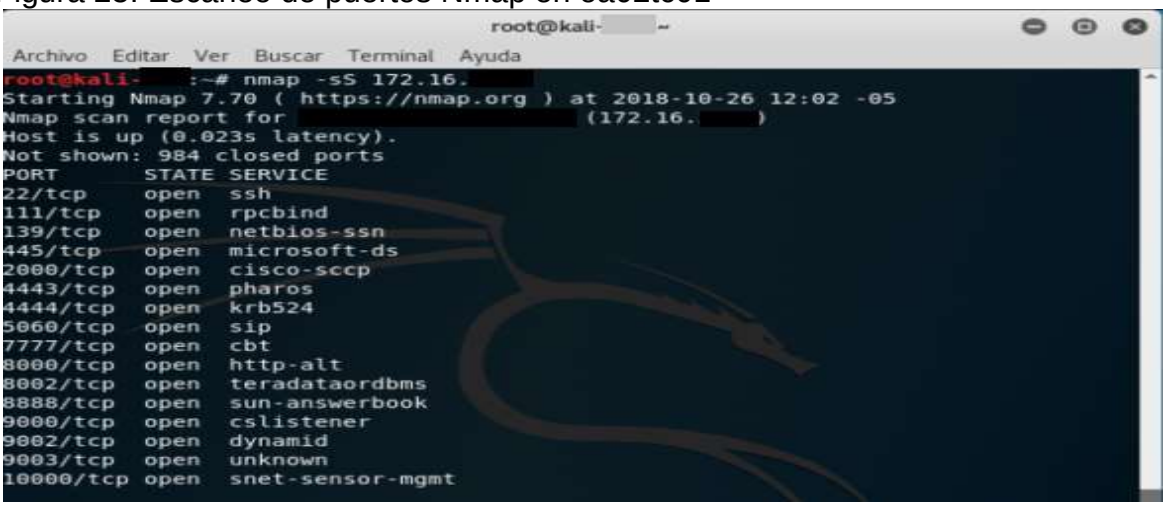


Fuente: Propiedad del Autor

4.2.3.2 Escaneo de puertos en publiquemos 2 host: oa02tc01 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 25. Escaneo de puertos Nmap en oa02tc01

Figura 25. Escaneo de puertos Nmap en oa02tc01

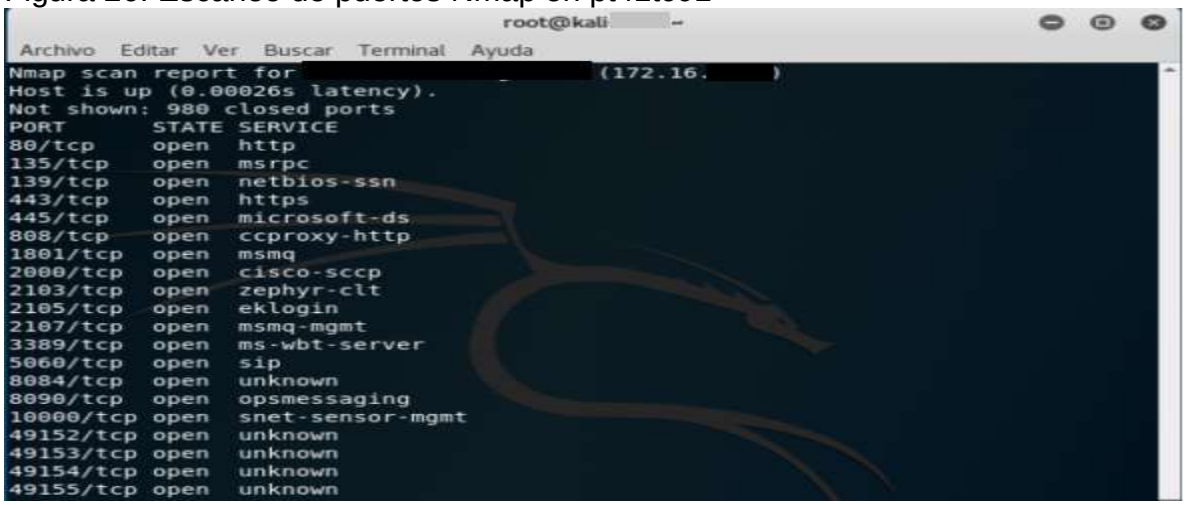


Fuente: Propiedad del Autor

4.2.3.3 Escaneo de puertos en aplicaciones kactus host: pt41tc01 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 26. Escaneo de puertos Nmap en pt41tc01

Figura 26. Escaneo de puertos Nmap en pt41tc01

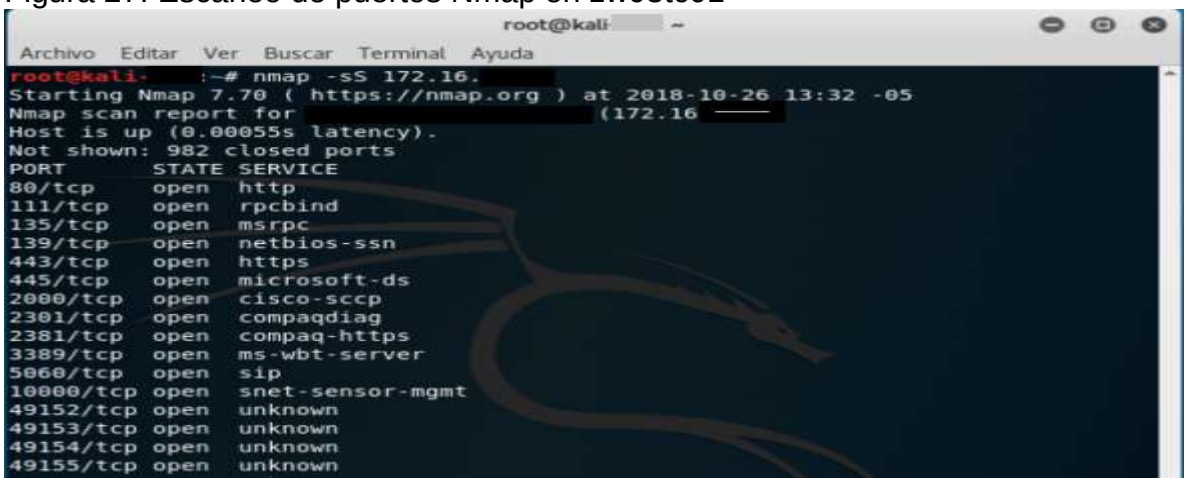


Fuente: Propiedad del Autor

4.2.3.4 Escaneo de puertos en producción base de datos kactus host: zw03tc01 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 27. Escaneo de puertos Nmap en zw03tc01

Figura 27. Escaneo de puertos Nmap en zw03tc01

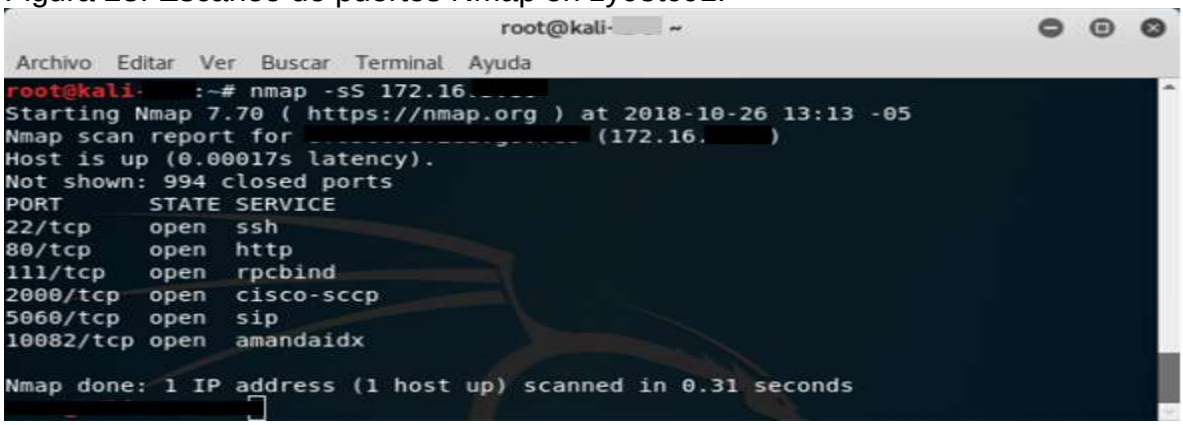


Fuente: Propiedad del Autor.

4.2.3.5 Escaneo de puertos en Morfeus host: zy03tc01 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 28. Escaneo de puertos Nmap en zy03tc01.

Figura 28. Escaneo de puertos Nmap en zy03tc01.

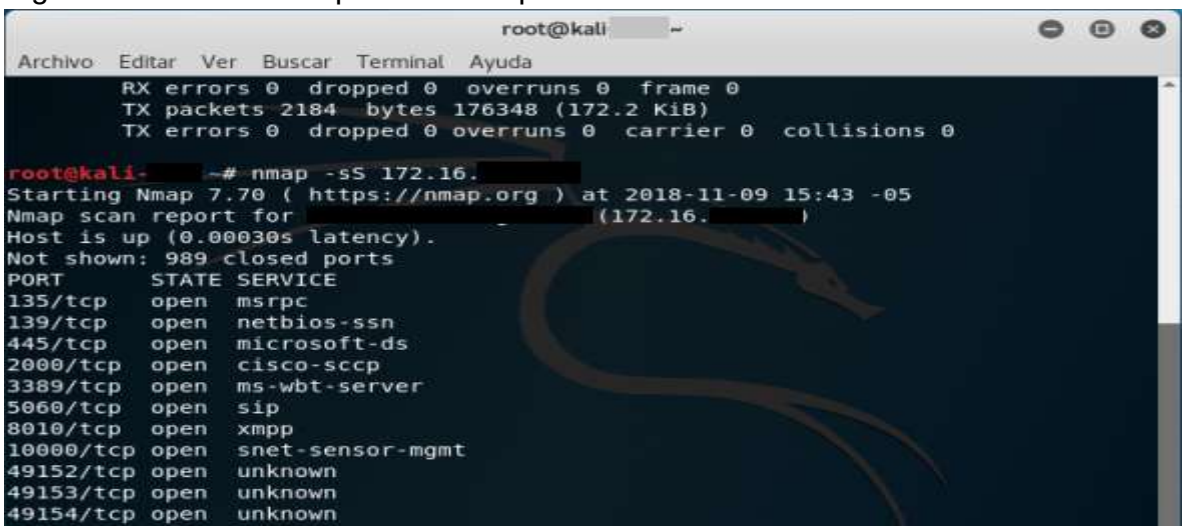


Fuente: Propiedad del Autor.

4.2.3.6 Escaneo de puertos en el servidor de aplicaciones sica host: zr03tc01 ip: 172.16.x.x.

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 29. Escaneo de puertos Nmap en zr03tc01

Figura 29. Escaneo de puertos Nmap en zr03tc01.

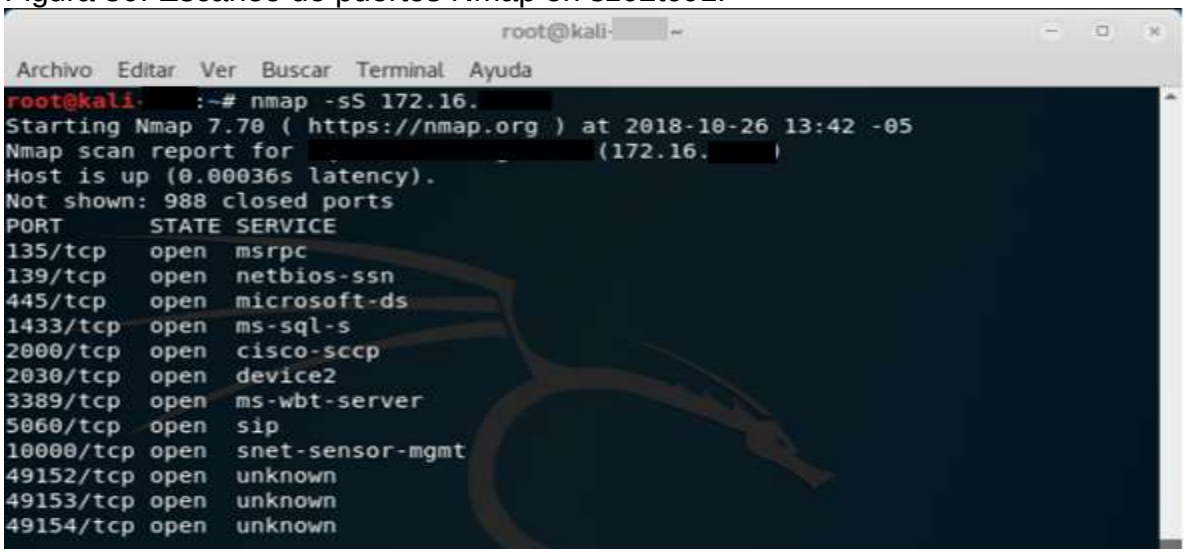


Fuente: Propiedad del Autor.

4.2.3.7 Escaneo de puertos en el repositorio base de datos sica host: sz02tc01 ip: 172.16.x.x.

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 30. Escaneo de puertos Nmap en sz02tc01

Figura 30. Escaneo de puertos Nmap en sz02tc01.

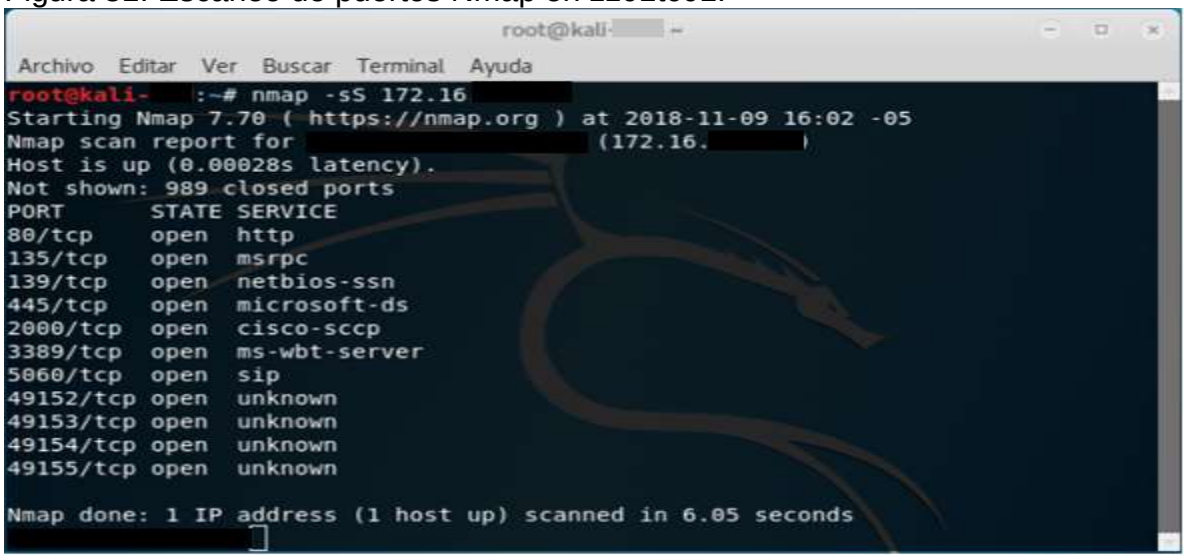


Fuente: Propiedad del Autor.

4.2.3.8 Escaneo de puertos en producción jones host: zz01tc01 ip: 172.16.x.x

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios efectuados por nmap como se muestra en la figura 31. Escaneo de puertos Nmap en zz01tc01

Figura 31. Escaneo de puertos Nmap en zz01tc01.



Fuente: Propiedad del Autor.

5. ANÁLISIS DE VULNERABILIDADES IDENTIFICADAS EN LA ORGANIZACIÓN CASO ESTUDIO.

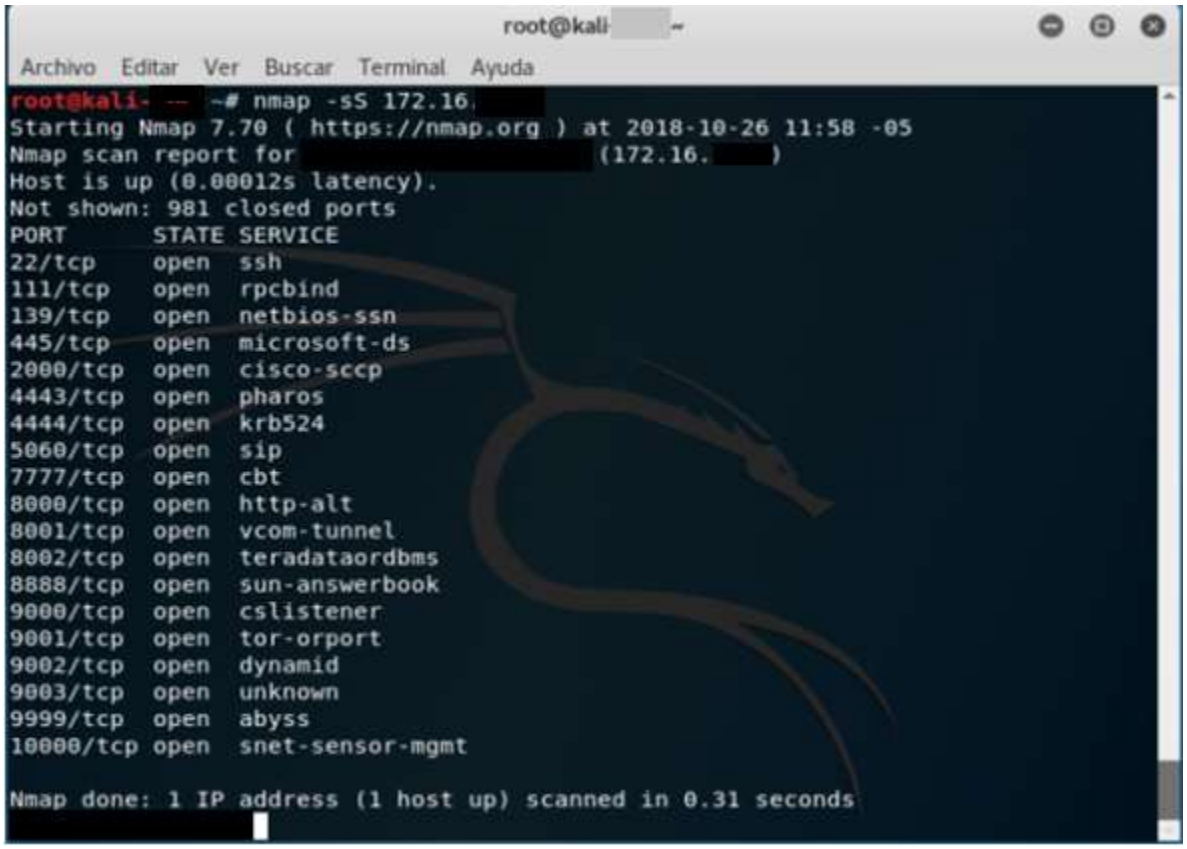
Se presenta el análisis de vulnerabilidades y servicios de puertos de cada uno de los host, como se aprecia a continuación:

5.1 PUBLIQUEMOS 1 HOST: OA11TC02 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que el puerto 9003/TCP en estado desconocido como se muestra en la figura 32. Escaneo de puertos Nmap en oa11tc01.

Figura 32. Escaneo de puertos Nmap en oa11tc01



Fuente: Propiedad del Autor

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de

severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 33. Información del Host oa11tc01

Fuente: Propiedad del Autor

5.1.1 Vulnerabilidad de Severidad Crítica del Host oa11tc01: 1.

El host oa11tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 26. Severidad critica del host oa11tc01

Tabla 26. Severidad Crítica del host oa11tc01

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor

- El host remoto ejecuta una versión no compatible de un servidor WebLogic.

  Según la versión, la instalación de Oracle WebLogic ejecutándose en el host remoto ya no es compatible. La falta de soporte implica que no lanzará nuevos parches de seguridad para el producto. Como resultado de ello, es probable que contenga vulnerabilidades de seguridad.

5.1.2 Vulnerabilidad de Severidad Alta del Host oa11tc01: 1

El host oa11tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 27. Severidad alta del host oa11tc01

Tabla 27. Severidad Alta del host oa11tc01

HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor

- El servidor remoto Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución de código remoto.

El servidor remoto Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución de código remoto en los componentes principales debido a la publicación por entregas insegura de objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java creado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.

5.1.3 Vulnerabilidad de Severidad Media del Host oa11tc01: 6

El host oa11tc01 presenta seis vulnerabilidades que requieren atención de tipo estándar, como se muestra en la tabla 28. Severidad media del host oa01tc01

Tabla 28. Severidad Media del host oa11tc01

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor

- No es necesario firmar en el servidor SMB remoto.

  Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

  El atributo 'commonName' (CN) del certificado SSL presentado para este

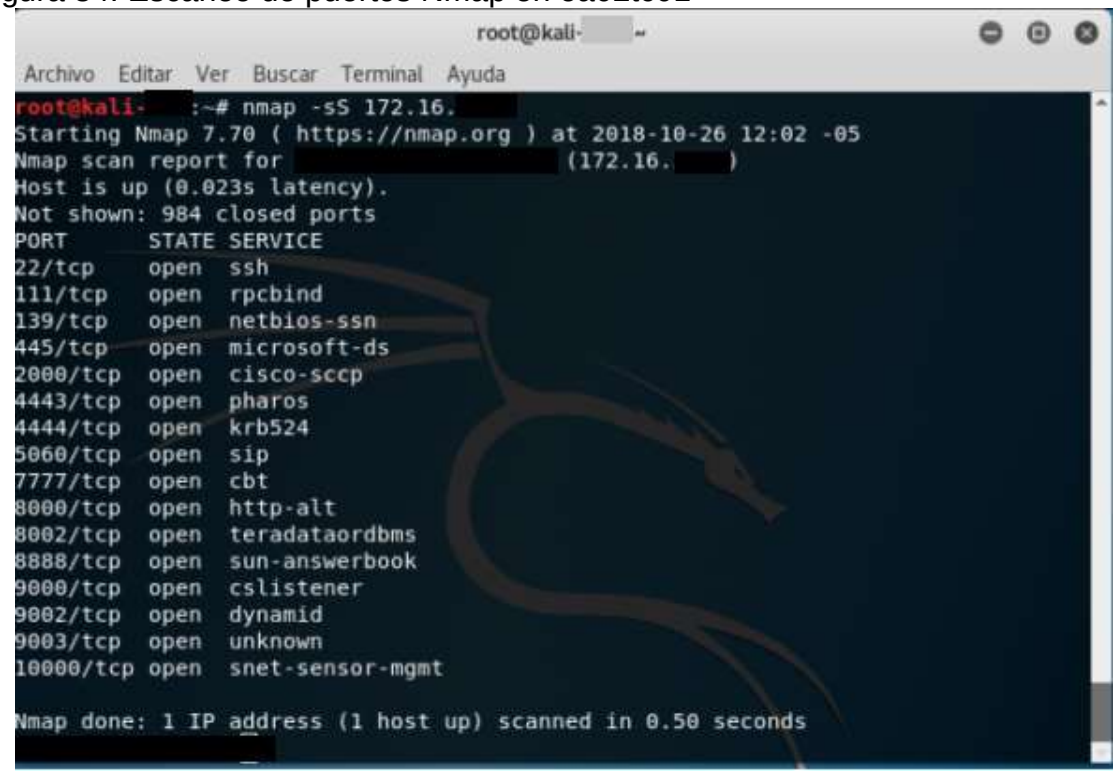
servicio es para una máquina diferente.

5.2 PUBLIQUEMOS 2 HOST: OA02TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia el puerto 9003/TCP en estado desconocido como se muestra en la figura 34. Escaneo de puertos Nmap en oa02tc01

Figura 34. Escaneo de puertos Nmap en oa02tc01



Fuente: Propiedad del Autor

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 35. Información del Host oa02tc01

Fuente: Propiedad del Autor

5.2.1 Vulnerabilidad de Severidad Crítica del Host oa02tc01: 1

El host oa02tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 29. Severidad critica del host oa02tc01

Tabla 29. Severidad Crítica del host oa02tc01

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor

- El host remoto ejecuta una versión no compatible de un servidor WebLogic.

  Según su versión, la instalación de Oracle WebLogic ejecutándose en el host remoto ya no es compatible. La falta de soporte implica que no lanzará nuevos parches de seguridad para el producto. Como resultado de ello, es probable que contenga vulnerabilidades de seguridad.

5.2.2 Vulnerabilidad de Severidad Alta del Host oa02tc01: 1

El host oa02tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 30. Severidad alta del host oa02tc01

Tabla 30. Severidad Alta del host oa02tc01

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.
  Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

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

5.2.3 Vulnerabilidad de Severidad Media del Host oa02tc01: 6

El host oa02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 31. Severidad Alta del host oa01tc01

Tabla 31. Severidad Crítica del host oa02tc01

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.
  Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

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

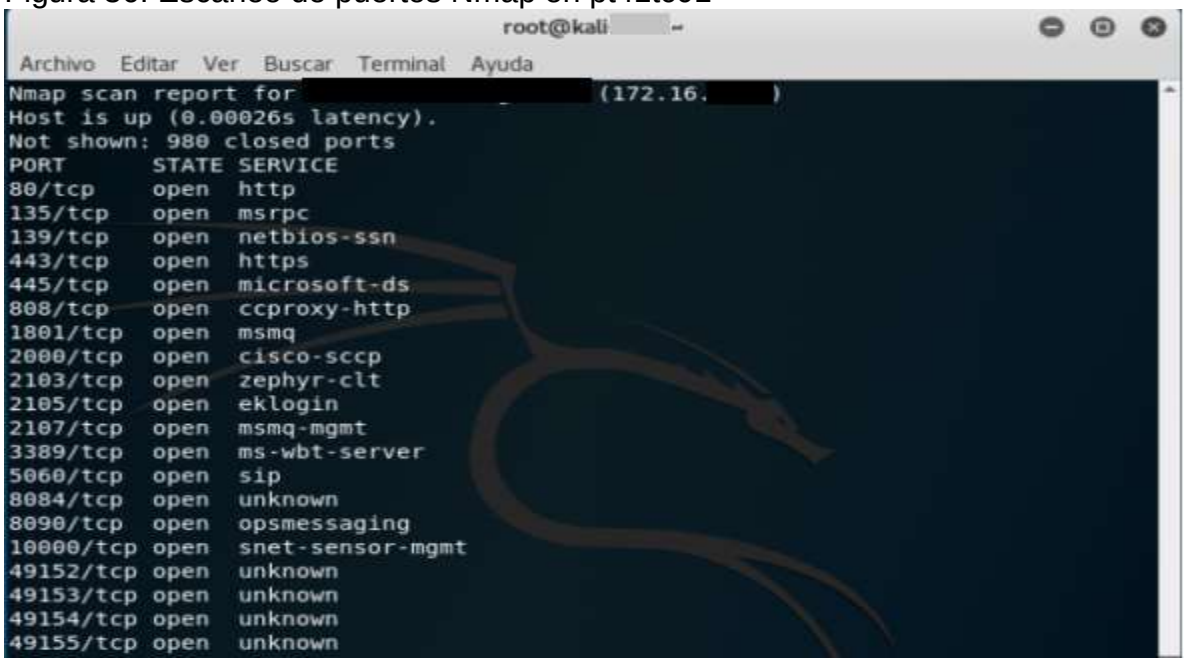
5.3 APLICACIONES KACTUS HOST: PT41TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia los puertos 8084/TCP, 49152/TCP,

49153/TCP, 49154/TCP, 49155/TCP en estados desconocidos como se muestra en la figura 36. Escaneo de puertos Nmap en pt41tc01

Figura 36. Escaneo de puertos Nmap en pt41tc01



Fuente: Propiedad del Autor

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 37. Información del Host pt41tc01

Fuente: Propiedad del Autor

5.3.1 Vulnerabilidad de Severidad Crítica del Host pt41tc01: 2

El host pt41tc01 presenta dos vulnerabilidades de alto grado de impacto, como se muestra en la tabla 32. Severidad critica del host pt41tc01

Tabla 32. Severidad Crítica del host pt41tc01

SEVERITY	CVSS	PLUGIN	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)

Fuente: Propiedad del Autor

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de por el paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados para un servidor Windows.
  Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje de Certificate Verify.
  Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente para el que no se ha solicitado mediante un mensaje CertificateRequest. En este caso, el plugin no puede proceder a la detección de la vulnerabilidad ya que el plugin No se puede enviar el mensaje de CertificateVerify.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de sistema.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad en (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC). Un ataque man-in-the-middle capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una

base de datos SAM que se pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

5.3.2 Vulnerabilidad de Severidad Crítica del Host pt41tc01: 1

El host pt41tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 33. Severidad alta del host pt41tc01

Tabla 33. Severidad Alta del host pt41tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas. El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por defectos criptográficos, incluyendo:

  Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques de hombre en el medio o para descifrar comunicaciones entre el servicio y los clientes afectados.

  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo (de modo que estas versiones sólo se utilizarán si el cliente o el servidor no soportan), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

5.3.3 Vulnerabilidad de Severidad Media del Host pt41tc01: 9

El host pt41tc01 presenta nueve vulnerabilidades que requieren atención de tipo estándar, como se muestra en la tabla 34. Severidad media del host pt41tc01.

Tabla 34. Severidad Media del host pt41tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- El certificado SSL del servidor remoto ha expirado.

  Este plugin comprueba las fechas de caducidad de los certificados asociados a los servicios SSL en el equipo de destino e informa si alguno ya ha expirado.
- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (Por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado. Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017, son considerados vulnerables.
- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

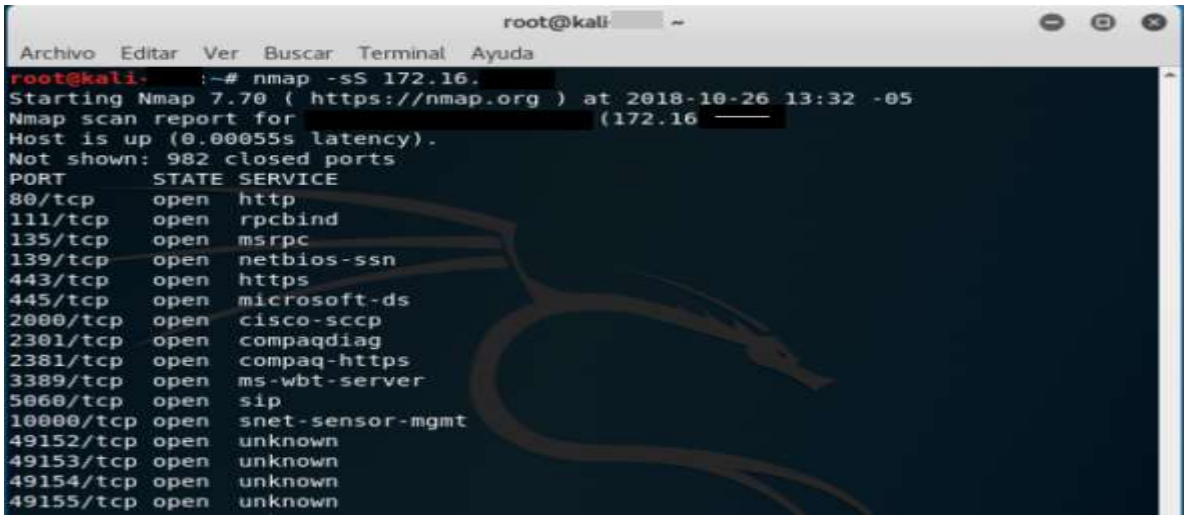
  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se considera de fuerza media a cualquier encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.
  Tenga en cuenta que es considerablemente más fácil eludir la encriptación de fuerza media si el atacante está en la misma red física.

5.4 PRODUCCIÓN BASE DE DATOS KACTUS HOST: ZW03TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, 49155/TCP, son de estados desconocidos como se muestra en la figura 38. Escaneo de puertos Nmap en zw03tc01

Figura 38. Escaneo de puertos Nmap en zw03tc01



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta

Nessus:
Figura 39. Información del Host zw03tc01

Fuente: Propiedad del Autor

5.4.1 Vulnerabilidad Severidad Crítica del Host zw03tc01: 4.

El host zw03tc01 presenta cuatro vulnerabilidades de alto grado de impacto, como se muestra en la tabla 11. Severidad critica del host zw03tc01.

Tabla 35. Severidad Crítica del host zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	94654	HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy)
CRITICAL	10.0	91222	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)
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)

Fuente: Propiedad del Autor.

- El servidor web remoto se ve afectado por múltiples vulnerabilidades. Según su banner, la versión de HP System Management Homepage (SMH) alojada en la web remota es anterior a 7.6. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

  En OpenSSL existe una condición de desbordamiento de búfer en heap en la función EVP_EncodeUpdate() dentro del archivo crypto/evp/encode.c que se activa al manejar una gran cantidad de datos de entrada. Un atacante remoto no autenticado puede explotar esto para causar una condición de negación de servicio.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por

una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de sistema.

5.4.2 Vulnerabilidad de Severidad Alta del Host zw03tc01: 1.

El host zw03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 36. Severidad Alta del host zw03tc01.

Tabla 36. Severidad Alta del host zw03tc01

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.8	103530	HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753)

Fuente: Propiedad del Autor.

- El servidor web remoto se ve afectado por múltiples vulnerabilidades.

  La versión de la página principal de gestión del sistema HP (SMH) alojada en el servidor web remoto es anterior a la versión 7.6.1. Por lo tanto, se ve afectado por múltiples vulnerabilidades, incluyendo múltiples vulnerabilidades de ejecución de código local y remoto.

5.4.3 Vulnerabilidad de Severidad Media del Host zw03tc01: 10

El host zw03tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 37. Severidad media del host zw03tc01

Tabla 37. Severidad Media del host: zw03tc01

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad

de privilegios.

El host Windows remoto se ve afectado por una vulnerabilidad de privilegios elevados en los protocolos de authority (Política de dominio) (LSAD) del administrador de cuentas de seguridad debido a un nivel de autenticación inadecuada negociación sobre los canales de llamada de procedimiento Remoto (RPC). Un atacante capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM que se puede explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- Puede ser posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-the middle (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación. Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

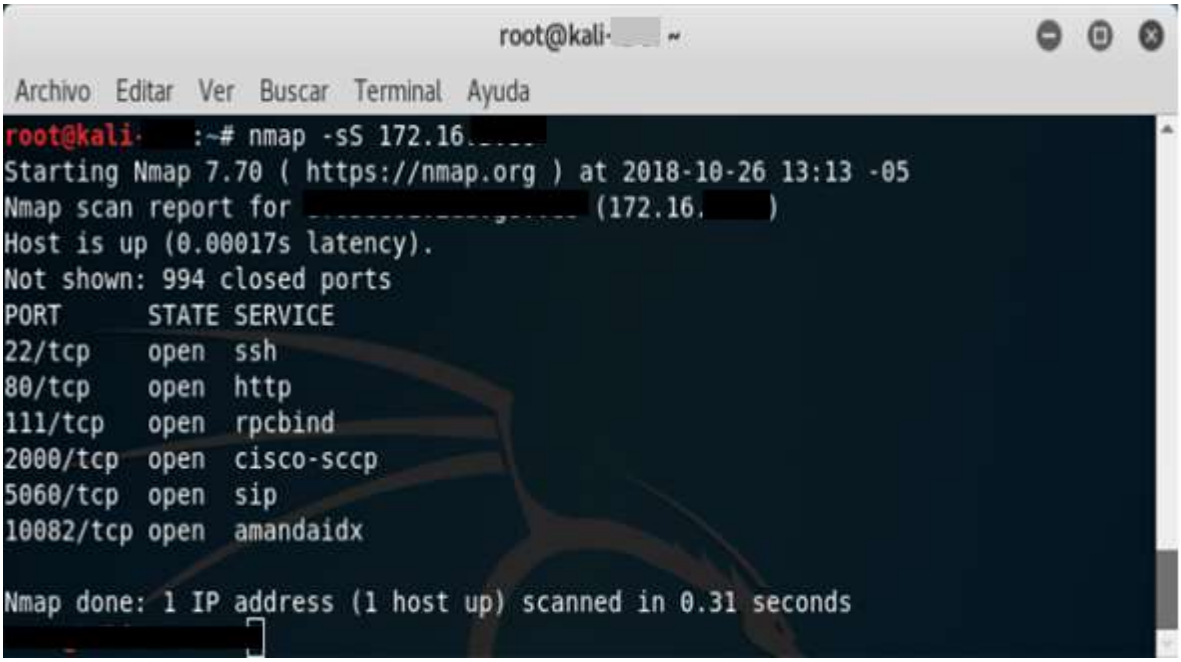
  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se considera de fuerza media a cualquier encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.
  Tenga en cuenta que es considerablemente más fácil eludir la encriptación de fuerza media si el atacante está en la misma red física.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

5.5 MORFEUS HOST: ZY03TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.
En los puertos de servicios, se evidencia que no existen puertos desconocidos como se muestra en la Figura 40. Escaneo de puertos Nmap zy03tc01.

Figura 40. Escaneo de puertos Nmap en zy03tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 41. Información del Host en zy03tc01

Fuente: Propiedad del Autor

5.5.1 Vulnerabilidad de Severidad Crítica del Host zy03tc01: 0

- En el en zy03tc01 no se encontró ninguna severidad crítica que pueda comprometer el host.

5.5.2 Vulnerabilidad de Severidad Alta del Host zy03tc01: 1

El host zy03tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 38. Severidad Alta del host zy03tc01.

Tabla 38. Severidad Alta del host en zy03tc01

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas.

- El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por varios defectos criptográficos, Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques para descifrar comunicaciones entre el servicio y los clientes afectados.
  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo, muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

5.5.3 Vulnerabilidad de Severidad Media del Host zy03tc01: 7.

El host zy03tc01 presenta siete vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 39. Severidad media del host zy03tc01

Tabla 39. Severidad Media del host en zy03tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

- Las funciones de depuración están habilitadas en el servidor web remoto.

El servidor web remoto soporta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidores web.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL del servidor remoto ya ha expirado.

  Este plugin comprueba las fechas de caducidad de los certificados asociados a los servicios SSL en el equipo de destino e informa si alguno ya ha caducado.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a las colisiones ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado.
  Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerable.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

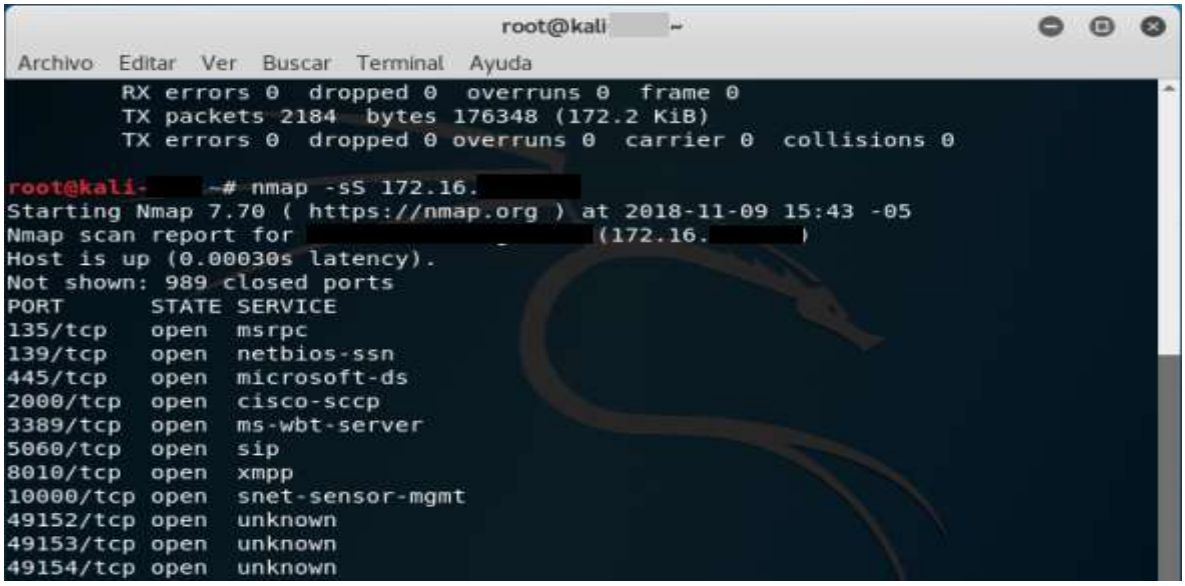
  La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
  Tenga en cuenta que este plugin no comprueba las cadenas de certificados que terminan en un certificado que no es autofirmado, sino que es firmado por una autoridad de certificación no reconocida.

5.6 SERVIDOR DE APLICACIONES SICA HOST: ZR03TC01 IP: 172.16.X.X.

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, son de estados desconocidos como se muestra en la figura 42. Escaneo de puertos Nmap en zr03tc01.

Figura 42. Escaneo de puertos Nmap en zr03tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 43. Información del Host zr03tc01.

Fuente: Propiedad del Autor.

5.6.1 Vulnerabilidad de Severidad Crítica del Host zr03tc01: 3

El host zr03tc01 presenta tres vulnerabilidades de alto grado de impacto, como se muestra en la tabla 40. Severidad critica del host zr03tc01.

Tabla 40. Severidad Crítica del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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	108797	Unsupported Windows OS

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de paquetes por parte del paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados a un servidor Windows.
  Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje vertificateVerify. Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente para el que no se ha solicitado un mensaje CertificateRequest.

- El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

  En Microsoft Server Message Block 1.0 (SMBv1) existen múltiples vulnerabilidades de ejecución de código remoto debido al tratamiento inadecuado de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).
  Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147).

- El sistema operativo remoto o service pack ya no es compatible.

  A la versión remota de Microsoft Windows le falta un Service Pack o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

5.6.2 Vulnerabilidad de Severidad Alta del Host zr03tc01: 1.

El host zr03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 41. Severidad Alta del host zr03tc01.

Tabla 41. Severidad Alta del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Fuente: Propiedad del Autor.

- El host remoto de Windows podría permitir la ejecución arbitraria de código.

  Existe una vulnerabilidad arbitraria de código remoto en la implementación del Protocolo de Escritorio Remoto (RDP) en el directorio host Windows remoto. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en memoria que ha sido se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta opción para hacer que el sistema ejecute código arbitrario enviando una secuencia de RDP. Este plugin también comprueba si existe una vulnerabilidad de denegación de servicio en Microsoft Terminal Server. Tenga en cuenta que este script no detecta la vulnerabilidad si la opción Permitir conexiones sólo desde equipos que se ejecutan la configuración de "Escritorio remoto con autenticación a nivel de red" está activada o la capa de seguridad está establecida en "SSL (TLS 1.0)' en el host remoto.

5.6.3 Vulnerabilidad de Severidad Media del Host zr03tc01: 9.

El host zr03tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 42. Severidad media del host zr03tc01.

Tabla 42. Severidad Media del host zr03tc01

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad, (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC).
  Un ataque man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- Puede ser posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-themiddle (MiTM) . El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.
  Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a las colisiones ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado.
  Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017.

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se recomienda la encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

  La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

- El Terminal Services remoto no utiliza únicamente autenticación a nivel de red.

  El Terminal Services remoto no está configurado para utilizar únicamente autenticación a nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para llevar a cabo la autenticación de servidores mediante mecanismos TLS/SSL o Kerberos, que protegen contra los ataques del tipo "man-in-the-middle". Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios y software maliciosos al completar la autenticación de usuario antes de que se establezca una conexión RDP completa.

- El host remoto está usando criptografía débil.

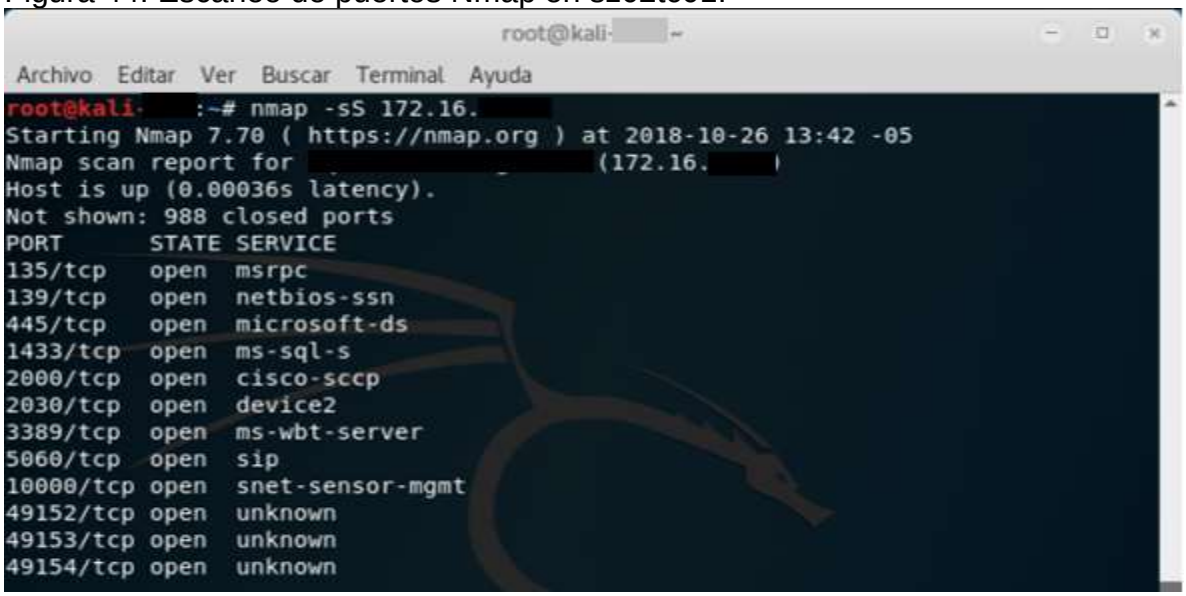
  El uso de criptografía débil con este servicio puede permitir que un atacante escuche las comunicaciones más fácilmente y obtenga capturas de pantalla y/o pulsaciones de teclas.

5.7 REPOSITORIO BASE DE DATOS SICA HOST: SZ02TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, son de estados desconocidos como se muestra en la figura 44. Escaneo de puertos Nmap en sz02tc01.

Figura 44. Escaneo de puertos Nmap en sz02tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 45. Información del Host sz02tc01.

Fuente: Propiedad del Autor.

5.7.1 Vulnerabilidad de Severidad Crítica del Host sz02tc01: 2.

El host sz02tc01 presenta dos vulnerabilidades de alto grado de impacto, como se muestra en la tabla 43. Severidad critica del host sz02tc01.

Tabla 43. Severidad Crítica del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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)

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de por el paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados para un servidor Windows. Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje de CertificateVerify.

- El host Windows remoto se ve afectado por las siguientes vulnerabilidades:

  En Microsoft Server Message Block 1.0 (SMBv1) existen múltiples vulnerabilidades de ejecución de código remoto debido al tratamiento inadecuado de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.

  Existe una vulnerabilidad de revelación de información en Microsoft Server Message Block 1.0 (SMBv1) debido en la tramitación de determinadas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial.

5.7.2 Vulnerabilidad de Severidad Alta del Host sz02tc01: 2.

El host sz02tc01 presenta dos vulnerabilidades que requiere atención de inmediata, como se muestra en la tabla 44. Severidad Alta del host sz02tc01

Tabla 44. Severidad Alta del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El host remoto de Windows podría permitir la ejecución arbitraria de código.

  Existe una vulnerabilidad arbitraria de código remoto en la implementación del Protocolo de Escritorio Remoto (RDP) en el directorio host Windows remoto. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en memoria que ha sido se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta opción. Para hacer que el sistema ejecute código arbitrario enviando una secuencia de RDP especialmente diseñada de paquetes. Este plugin también comprueba si existe una vulnerabilidad de denegación de servicio en Microsoft Terminal Server.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas. El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por varios defectos criptográficos:

  Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques de hombre en el medio o para descifrar comunicaciones entre el servicio y los clientes afectados.
  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo (de modo que estas versiones sólo se utilizarán si el cliente o el servidor no soportan nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

5.7.3 Vulnerabilidad de Severidad Media del Host sz02tc01: 11.

El host sz02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 45. Severidad media del host sz02tc01

Tabla 45. Severidad Media del host sz02tc01

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Fuente: Propiedad del Autor

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad. (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación por procedimiento Remoto (RPC). Un atacante man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM, pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.
- Es posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-themiddle (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación.
  Un atacante con la capacidad de interceptar tráfico desde el servidor RDP, puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.

Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a este tipo de ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite a un atacante para que se haga pasar por el servicio afectado.
- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.
  El host remoto soporta el uso de cifrados SSL con cifrado de fuerza media. Se considera de cambiar las longitudes de clave de al menos 64 bits o de 112 bits, o bien que utilice la suite de encriptación 3DES.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

  La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

- Es posible obtener información sensible del host remoto con servicios habilitados para SSL/TLS.

  El host remoto se ve afectado por una vulnerabilidad de revelación de información de hombre en el medio (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno

al descifrar los mensajes.

- Fue posible obtener información sensible del host remoto con los servicios habilitados para TLS.

  El host remoto se ve afectado por una vulnerabilidad de revelación de información de hombre en el medio (MitM) conocida como POODLE. La vulnerabilidad se debe a que el servidor TLS no verifica el relleno de cifrado por bloques cuando utiliza un conjunto de como AES y DES. La falta de comprobación de relleno puede permitir descifrar el tráfico TLS cifrado. Esta vulnerabilidad podría permitir el descifrado del tráfico HTTPS por un tercero no autorizado.

- El host remoto está usando criptografía débil.

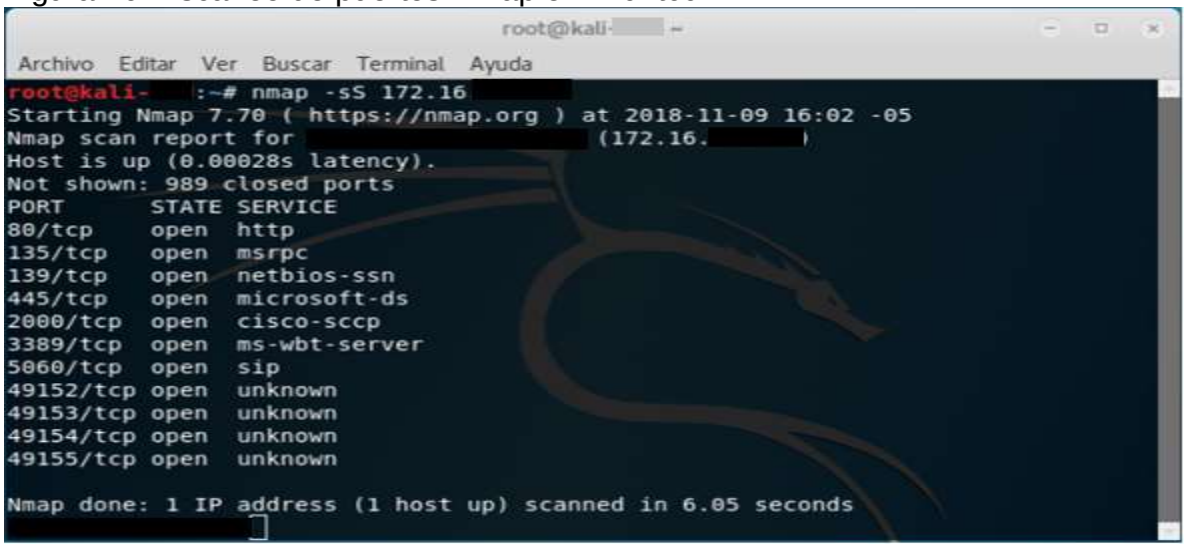
  El servicio de Terminal Services remoto no está configurado para utilizar criptografía fuerte. El uso de criptografía débil con este servicio puede permitir a un atacante espiar las comunicaciones y obtener capturas de pantalla y/o pulsaciones de teclas.

5.8 PRODUCCIÓN JONES HOST: ZZ01TC01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia los puerto 49152/TCP, 49153/TCP, 49154/TCP, 49155/TCP, en estados desconocidos como se muestra en la figura 46. Escaneo de puertos Nmap en zz01tc01.

Figura 46. Escaneo de puertos Nmap en zz01tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 47. Información del Host zz01tc01.

Fuente: Propiedad del Autor.

5.8.1 Vulnerabilidad de Severidad Crítica del Host zz01tc01: 1.

El host zz01tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 46. Severidad critica del host zz01tc01.
Tabla 46. Severidad Crítica del host zz01tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un dispositivo remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de Sistema.

5.8.2 Vulnerabilidad de Severidad Alta del Host zz01tc01: 0.

- En el Host zz01tc01 no se encontró ninguna severidad crítica que pueda comprometer el host.

5.8.3 Vulnerabilidad de Severidad Media del Host zz01tc01: 9.

El host zz01tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 47. Severidad media del host zz01tc01.

Tabla 47. Severidad Media del host zz01tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el administrador cuentas de seguridad (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC). Un ataque man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos explotando y forzando el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques de man-in-themiddle (MiTM) el cliente RDP no realiza la validación de la identidad del servidor mediante encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.
  Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (Por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a las colisiones ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado. Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017.

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se recomienda la encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.

- El Terminal Services remoto no utiliza únicamente autenticación a nivel de red.

  El Terminal Services remoto no está configurado para utilizar únicamente autenticación a nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para llevar a cabo la autenticación de servidores mediante mecanismos TLS/SSL o Kerberos, que protegen contra los ataques del tipo "man-in-the-middle". Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios y software maliciosos al completar la autenticación de usuario antes de que se establezca una conexión RDP completa.

6. RECOMENDACIONES DE VULNERABILIDADES HALLADAS A LA ORGANIZACION CASO DE ESTUDIO.

6.1 INTRODUCCIÓN

En la organización caso de estudio, La información es uno de los activos más importantes, siendo esta una de las responsabilidades más grandes de los empleados de la organización caso estudio, por esta razón es indispensable adoptar los mecanismos esenciales para su protección en caso de un ataque informático.

Se hace necesario realizar un análisis de vulnerabilidades para identificar aquellas brechas de seguridad a las que se encuentran expuestas tanto externa e internamente la Institución. Este análisis de vulnerabilidades se realizará mediante escaneo de puertos activos y vulnerabilidades, en donde se aplican pruebas de "Pen Test" que son realizadas mediante metodologías de ética hacking con el uso de software y herramientas que son primordiales para este tipo de procedimiento.

Con este análisis se pretende disminuir y controlar los peligros existentes a los que se encuentran expuestos los host más críticos de la organización caso de estudio, así como también conocer la situación actual de seguridad con el fin de implementar medidas preventivas y correctivas con el fin mitigar dichos riesgos y amenazas.

6.2 OBJETIVOS.

6.2.1 Objetivo General.

Realizar análisis y escaneo de vulnerabilidades a la infraestructura Tecnológica de la organización caso de estudio

6.2.2 Objetivo Específicos.

- Recolección de información y selección de los host críticos de la organización caso estudio para monitorear y tener un control de inventario de las mismas.
- Analizar las vulnerabilidades identificadas, teniendo en cuenta su nivel de severidad en los host críticos de la organización caso estudio.
- Presentación de los servicios "Recomendaciones" que se implementara en la organización caso de estudio, detallando la ejecución.

6.3 ALCANCE.

El alcance del documento está relacionado con el análisis y hacking ético aplicado en los host más críticos de la organización caso estudio, este procedimiento fue realizado durante los meses de octubre y noviembre a los equipos asignados, con el fin de brindar recomendaciones de mitigación para los mismos.

6.4 GLOSARIO

- **Vulnerabilidad:** Debilidad de un elemento tecnológico que permite un comportamiento no deseado.
- **CVE:** Vulnerabilidades Comunes y Expuestas.
- **Exploit:** Fragmento de código desarrollado para aprovechar una vulnerabilidad especifica.
- **Severidad alta:** Vulnerabilidades que requieren atención inmediata.
- **Severidad media:** Vulnerabilidades que requieren atención de tipo estándar.
- **Severidad baja:** Vulnerabilidades que requieren atención después de atender eventos o incidentes con severidad alta y/o media.
- **Malware:** Software Malicioso o malintencionado diseñado para causar efectos no deseados en un dispositivo.
- **CBC:** Cifrado de bloques cambiante.
- **Arcfour:** Algoritmo de cifrado también conocido como RC4
- **Hash:** Algoritmo matemático usado para comprobar la autenticidad de un archivo o un dato.
- **Man-In-The-Middle (Mitm):** Ataque que permite a un atacante leer información, ubicándose en medio del origen y el destino de la información.
- **AES:** Estándar avanzado de encriptación.

6.5 ANALISIS DE VULNERABILIDADES DE LOS PRINCIPALES HOST CRITICOS DE LA ORGANIZACIÓN CASO ESTUDIO.

Mediante la ejecución de análisis de vulnerabilidades en los host es efectuado con el fin de incrementar la seguridad de aquellas brechas de vulnerabilidades que serán identificadas, con tal fin después sean mitigados por el grupo área del tecnología y cómputo de la organización caso de estudio de la organización caso de estudio.

A continuación se describe los servicios asignados que fueron analizados en la Tabla 1. Host críticos de la organización caso de estudio:

Tabla 48. Host Críticos de la Organización caso de estudio.

HOST CRITICOS DE LA ORGANIZACIÓN CASO ESTUDIO			
NOMBRE DE HOST	**HOST**	**DESCRIPCION**	**RESPONSABLE**
oa11tc01	172.16.x.x	Publiquemos 1	Infraestructura
oa02tc01	172.16.x.x	Publiquemos 2	Infraestructura
pt41tc01	172.16.x.x	Aplicaciones Kactus	Infraestructura
zw03tc01	172.16.x.x	Producción base de datos Kactus.	Infraestructura
zy03tc01	172.16.x.x	Morfeus	Infraestructura
zr03tc01	172.16.x.x	Servidor de aplicaciones SICA	Infraestructura

sz02tc01	172.16.x.x	Repositorio Base de datos SICA	Infraestructura
zz01tc01	172.16.x.x	Producción Jones	Infraestructura

Fuente: Propiedad del Autor

6.6 ANÁLISIS DE VULNERABILIDADES IDENTIFICADAS, TENIENDO EN CUENTA SU NIVEL DE SEVERIDAD EN LOS HOST CRÍTICOS DE LA ORGANIZACIÓN CASO DE ESTUDIO.

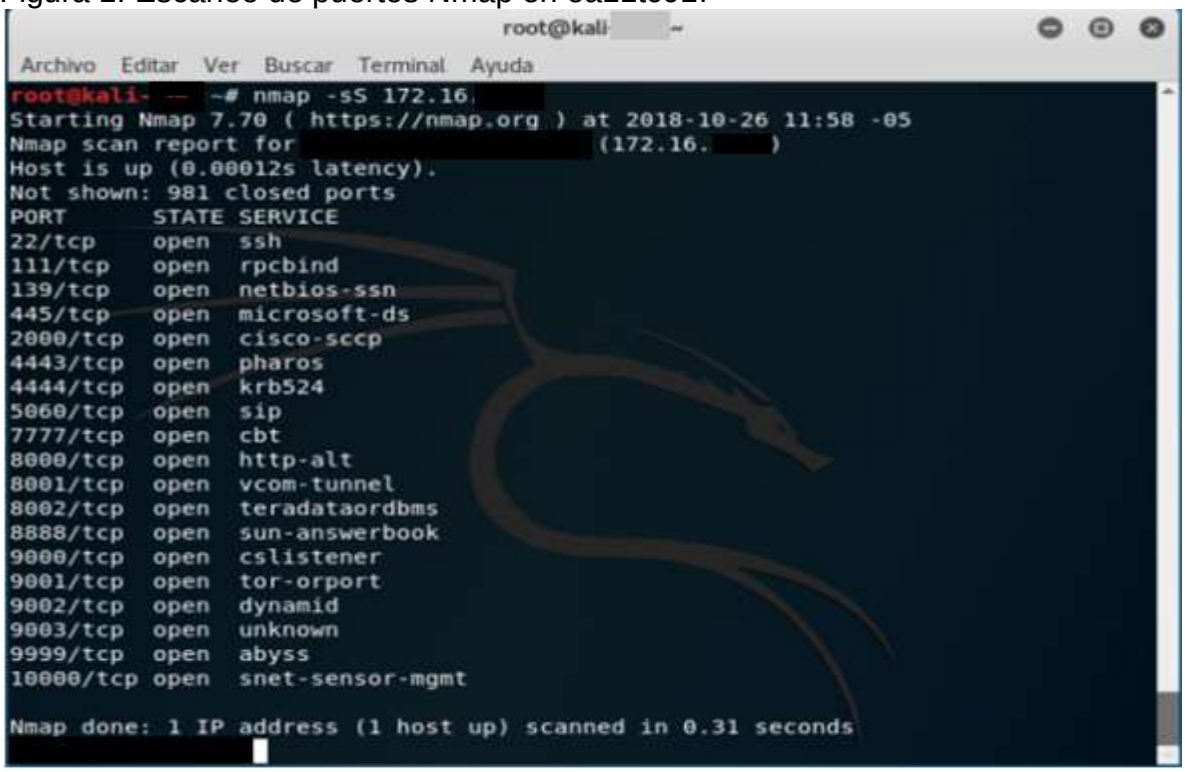
Se presenta el análisis de vulnerabilidades y servicios de puertos de cada uno de los host, como se aprecia a continuación:

6.6.1 Publiquemos 1 Host: oa11tc02 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que el puerto 9003/TCP en estado desconocido como se muestra en la figura 13. Escaneo de puertos Nmap en oa11tc01.

Figura 1. Escaneo de puertos Nmap en oa11tc01.

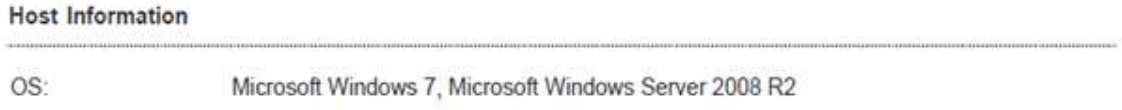


Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información

del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 2. Información del Host oa11tc01



Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 1

El host oa11tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 2. Severidad critica del host oa01tc01.

Tabla 2. Severidad Crítica del host oa01tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor.

- El host remoto ejecuta una versión no compatible de un servidor WebLogic.

  Según la versión, la instalación de Oracle WebLogic ejecutándose en el host remoto ya no es compatible. La falta de soporte implica que no lanzará nuevos parches de seguridad para el producto. Como resultado de ello, es probable que contenga vulnerabilidades de seguridad.

Vulnerabilidad de Severidad Alta: 1.

El host oa11tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 3. Severidad alta del host oa01tc01.

Tabla 3. Severidad Alta del host oa01tc01

HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor.

- El servidor remoto Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución de código remoto.

El servidor remoto Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución de código remoto en los componentes principales debido a la publicación por entregas insegura de objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java creado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Vulnerabilidad de Severidad Media: 6.

El host oa01tc01 presenta seis vulnerabilidades que requieren atención de tipo estándar, como se muestra en la tabla 4. Severidad media del host oa01tc01.
Tabla 4. Severidad Media del host oa01tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

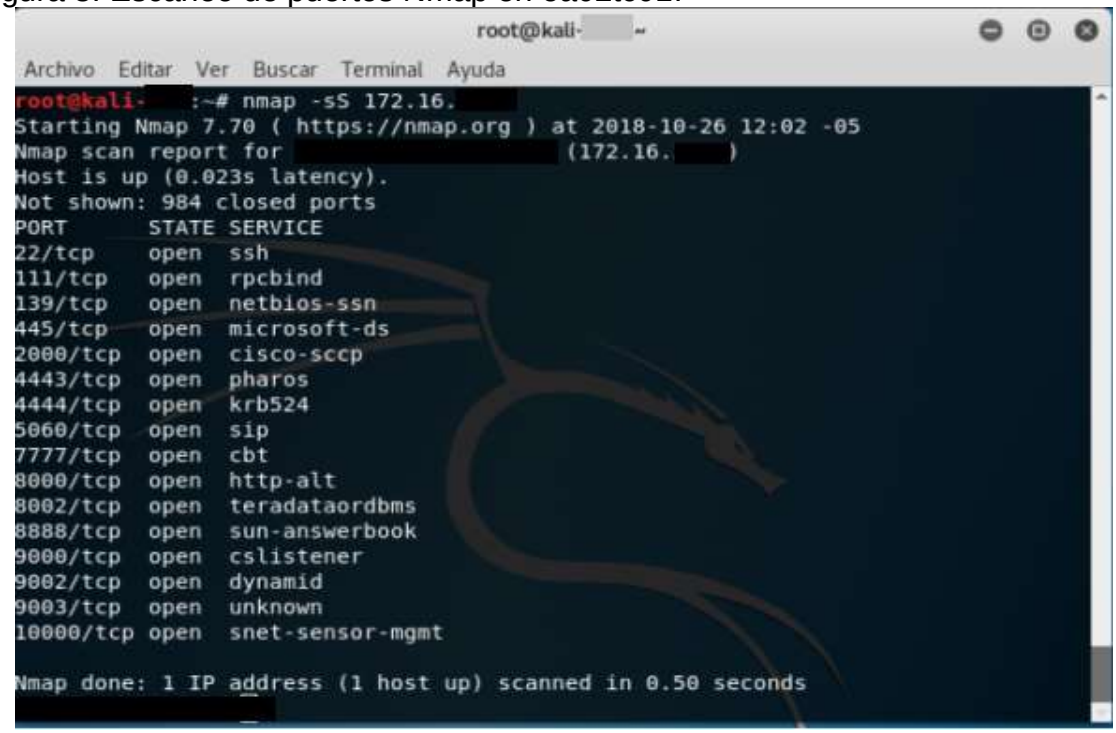
  El atributo 'common Name' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.

6.6.2 Publiquemos 2 Host: oa02tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que el puerto 9003/TCP en estado desconocido como se muestra en la figura 15. Escaneo de puertos Nmap en oa02tc01.

Figura 3. Escaneo de puertos Nmap en oa02tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 4. Información del Host oa02tc01.

Fuente: Propiedad del Autor

Vulnerabilidad de Severidad Crítica: 1.

El host oa02tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 5. Severidad critica del host oa02tc01.

Tabla 5. Severidad Crítica del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	109345	Oracle WebLogic Unsupported Version Detection

Fuente: Propiedad del Autor.

- El host remoto ejecuta una versión no compatible de un servidor WebLogic.

  Según su versión, la instalación de Oracle WebLogic ejecutándose en el host remoto ya no es compatible. La falta de soporte implica que no lanzará nuevos parches de seguridad para el producto. Como resultado de ello, es probable que contenga vulnerabilidades de seguridad.

Vulnerabilidad de Severidad Alta: 1

El host oa02tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 6. Severidad alta del host oa02tc01.

Tabla 6. Severidad Alta del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	111665	Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Fuente: Propiedad del Autor.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

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

Vulnerabilidad de Severidad Media: 6.

El host oa02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 7. Severidad Alta del host oa01tc01

Tabla 7. Severidad Crítica del host oa02tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

Fuente: Propiedad del Autor.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques de hombre en medio contra el servidor SMB.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL para este servicio es para un host diferente.

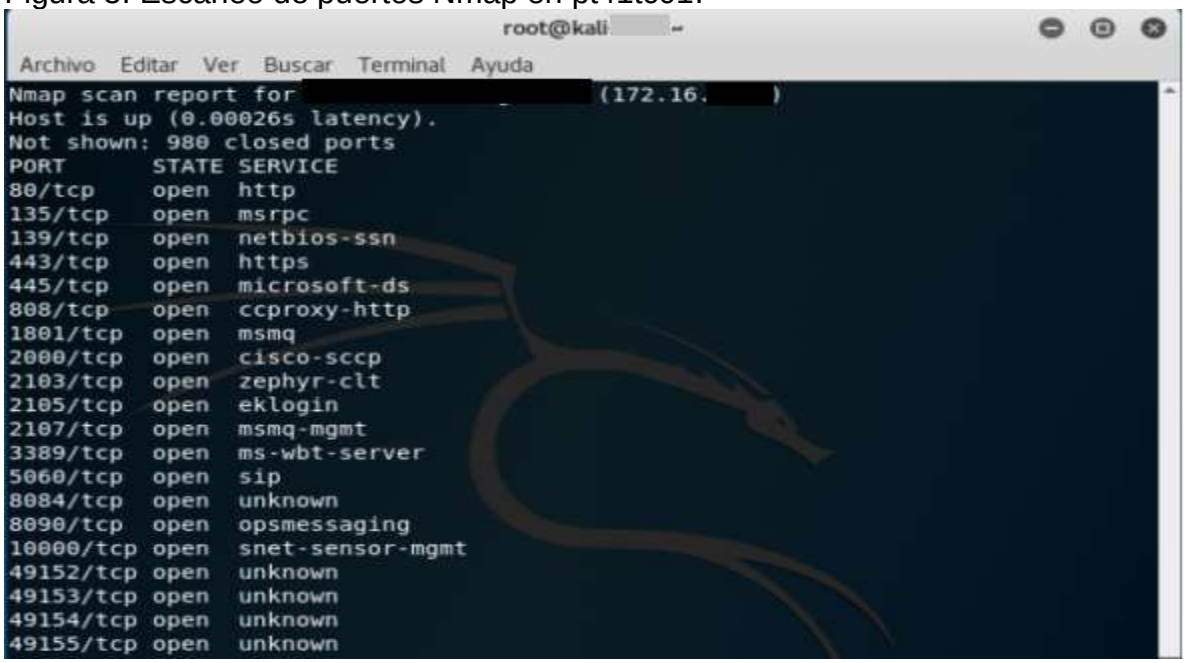
  El atributo 'common Name' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.

6.6.3 Aplicaciones Kactus Host: pt41tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, 49155/TCP son de estados desconocidos como se muestra en la figura 5. Escaneo de puertos Nmap en pt41tc01.

Figura 5. Escaneo de puertos Nmap en pt41tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 6. Información del Host pt41tc01.

Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 2

El host pt41tc01 presenta dos vulnerabilidades de alto grado de impacto, como se muestra en la tabla 8. Severidad critica del host pt41tc01.

Tabla 8. Severidad Crítica del host pt41tc01.

SEVERITY	CVSS	PLUGIN	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)

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de por el paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados para un servidor Windows.

  Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje de Certificate Verify.
  Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente para el que no se ha solicitado mediante un mensaje CertificateRequest. En este caso, el plugin no puede proceder a la detección de la vulnerabilidad ya que el plugin No se puede enviar el mensaje de CertificateVerify.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de sistema.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad en (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC). Un ataque man-in-the-middle capaz de

interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM que se pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

Vulnerabilidad de Severidad Crítica: 1.

El host pt41tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 9. Severidad alta del host pt41tc01.

Tabla 9. Severidad Alta del host pt41tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas. El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por defectos criptográficos, incluyendo:

  Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques de hombre en el medio o para descifrar comunicaciones entre el servicio y los clientes afectados.

  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo (de modo que estas versiones sólo se utilizarán si el cliente o el servidor no soportan), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

Vulnerabilidad de Severidad Media: 9.

El host pt41tc01 presenta nueve vulnerabilidades que requieren atención de tipo estándar, como se muestra en la tabla 10. Severidad media del host pt41tc01.

Tabla 10. Severidad Media del host pt41tc01

SEVERITY	CVSS	PLUGIN	NAME
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	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- El certificado SSL del servidor remoto ha expirado.

  Este plugin comprueba las fechas de caducidad de los certificados asociados a los servicios SSL en el equipo de destino e informa si alguno ya ha expirado.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (Por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado. Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017, son considerados vulnerables.

- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

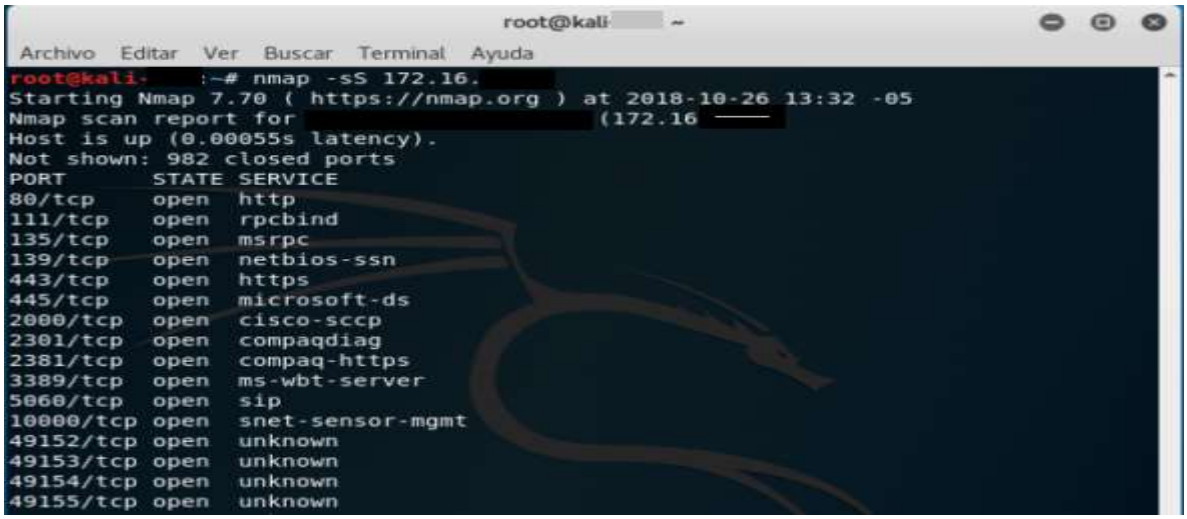
  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se considera de fuerza media a cualquier encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.
  Tenga en cuenta que es considerablemente más fácil eludir la encriptación de fuerza media si el atacante está en la misma red física.

6.6.4 Producción Base de Datos kactus Host: zw03tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, 49155/TCP, son de estados desconocidos como se muestra en la figura 19. Escaneo de puertos Nmap en zw03tc01

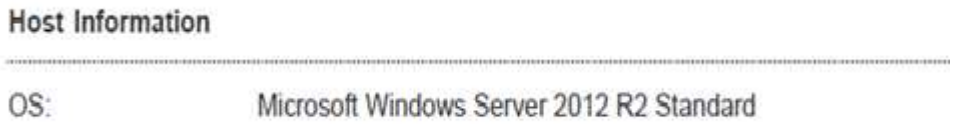
Figura 7. Escaneo de puertos Nmap en zw03tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 8. Información del Host zw03tc01



Fuente: Propiedad del Autor.

Vulnerabilidad Severidad Critica: 4.

El host zw03tc01 presenta cuatro vulnerabilidades de alto grado de impacto, como se muestra en la tabla 11. Severidad critica del host zw03tc01.

Tabla 11. Severidad Crítica del host zw03tc01

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	94654	HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy)
CRITICAL	10.0	91222	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)
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)

Fuente: Propiedad del Autor.

- El servidor web remoto se ve afectado por múltiples vulnerabilidades. Según su banner, la versión de HP System Management Homepage (SMH) alojada en la web remota es anterior a 7.6. Por lo tanto, se ve afectado por las siguientes vulnerabilidades:

  En OpenSSL existe una condición de desbordamiento de búfer en heap en la función EVP_EncodeUpdate() dentro del archivo crypto/evp/encode.c que se activa al manejar una gran cantidad de datos de entrada. Un atacante remoto no autenticado puede explotar esto para causar una condición de negación de servicio.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por

una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un atacante remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de sistema.

Vulnerabilidad de Severidad Alta: 1.

El host zw03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 12. Severidad Alta del host zw03tc01.

Tabla 12. Severidad Alta del host zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.8	103530	HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753)

Fuente: Propiedad del Autor.

- El servidor web remoto se ve afectado por múltiples vulnerabilidades.

  La versión de la página principal de gestión del sistema HP (SMH) alojada en el servidor web remoto es anterior a la versión 7.6.1. Por lo tanto, se ve afectado por múltiples vulnerabilidades, incluyendo múltiples vulnerabilidades de ejecución de código local y remoto.

Vulnerabilidad de Severidad Media: 10.

El host zw03tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 13. Severidad media del host zw03tc01.

Tabla 49. Severidad Media del host: zw03tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host Windows remoto se ve afectado por una vulnerabilidad de privilegios elevados en los protocolos de authority (Política de dominio) (LSAD) del Administrador de cuentas de seguridad debido a un nivel de autenticación inadecuada negociación sobre los canales de llamada de procedimiento Remoto (RPC). Un atacante capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM que se puede explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- Puede ser posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-the middle (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación. Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se considera de fuerza media a cualquier encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.
  Tenga en cuenta que es considerablemente más fácil eludir la encriptación de fuerza media si el atacante está en la misma red física.

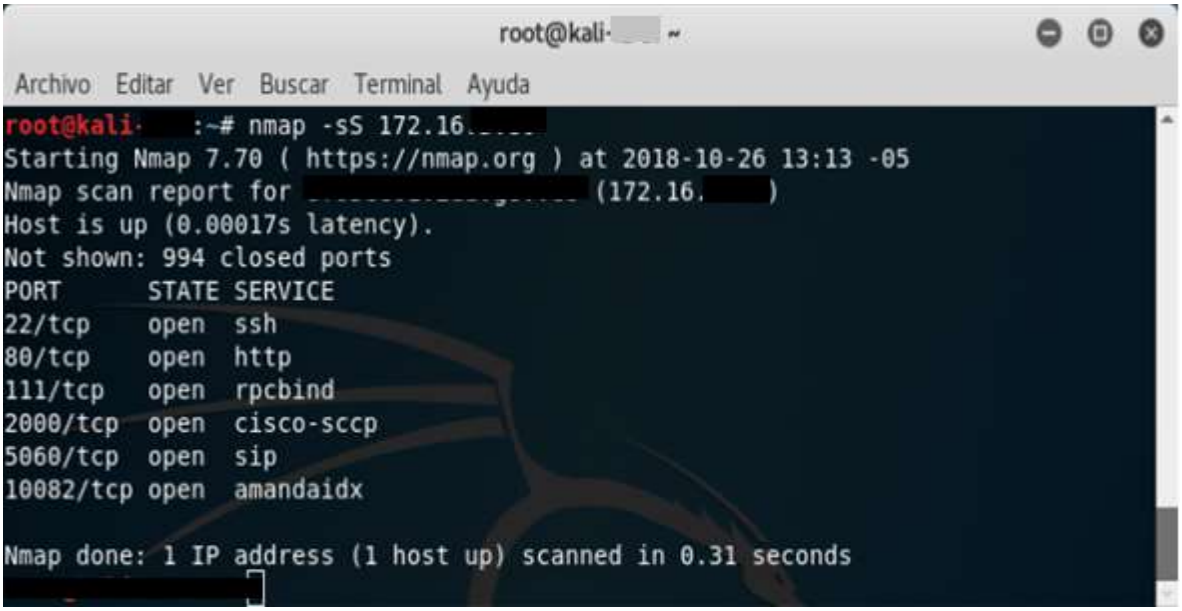
- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

6.6.5 Morfeus Host: zy03tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios con Nmap.

En los puertos de servicios, se evidencia que no existen puertos desconocidos como se muestra en la Figura 9. Escaneo de puertos Nmap zy03tc01.

Figura 9. Escaneo de puertos Nmap en zy03tc01.



Fuente: Propiedad del Autor.

Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 10. Información del Host en zy03tc01.

Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 0.

En el en zy03tc01 no se encontró ninguna severidad crítica que pueda comprometer el host.

Vulnerabilidad de Severidad Alta: 1.

El host zy03tc01 presenta una vulnerabilidad que requiere atención inmediata, como se muestra en la tabla 14. Severidad Alta del host zy03tc01.

Tabla 14. Severidad Alta del host en zy03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas.

- El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por varios defectos criptográficos, Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques para descifrar comunicaciones entre el servicio y los clientes afectados.
  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo, muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

Vulnerabilidad de Severidad Media: 7.

El host zy03tc01 presenta siete vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 15. Severidad media del host zy03tc01.
Tabla 15. Severidad Media del host en zy03tc01.

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Fuente: Propiedad del Autor.

- Las funciones de depuración están habilitadas en el servidor web remoto.

El servidor web remoto soporta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidores web.

- El servidor SSH remoto está configurado para permitir algoritmos de encriptación débiles o ningún algoritmo.

  Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o no tiene cifrado alguno. RFC 4253 aconseja no usar Arcfour debido a un problema con llaves débiles.

- El certificado SSL del servidor remoto ya ha expirado.

  Este plugin comprueba las fechas de caducidad de los certificados asociados a los servicios SSL en el equipo de destino e informa si alguno ya ha caducado.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado.
  Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerable.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

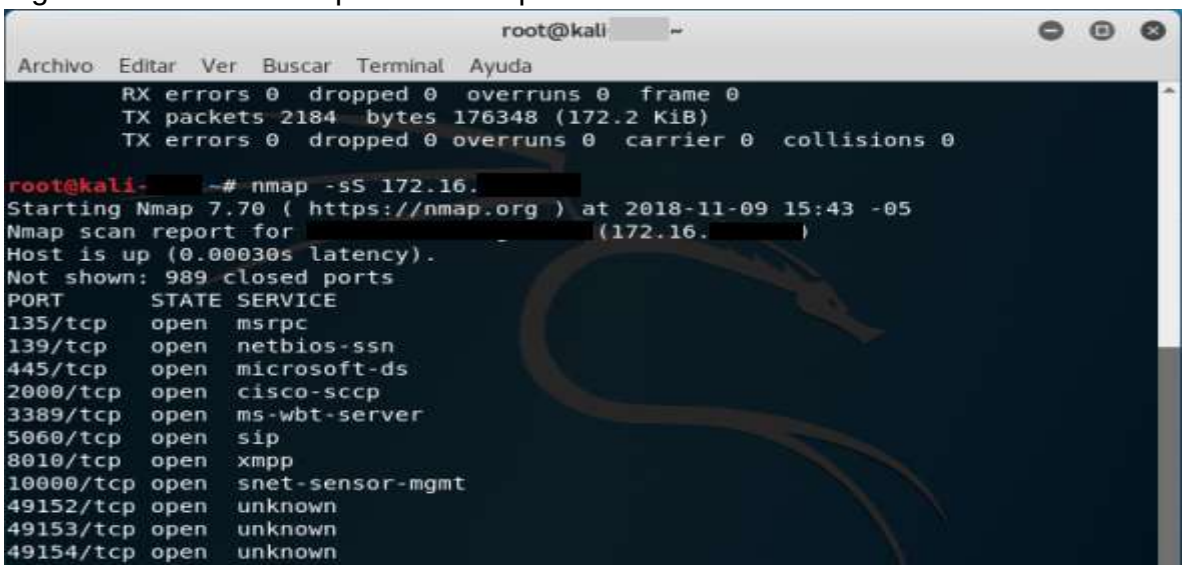
  La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
  Tenga en cuenta que este plugin no comprueba las cadenas de certificados que terminan en un certificado que no es autofirmado, sino que es firmado por una autoridad de certificación no reconocida.

6.6.6 Servidor de aplicaciones SICA Host: zr03tc01 IP: 172.16.X.X.

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, son de estados desconocidos como se muestra en la figura 11. Escaneo de puertos Nmap en zr03tc01.

Figura 11. Escaneo de puertos Nmap en zr03tc01.



Fuente: Propiedad del Autor.

Analiza los reportes del escaneo de vulnerabilidades con la herramienta Nessus, detallando la información del host y cada vulnerabilidad teniendo en cuenta las vulnerabilidades según el nivel de severidad (nivel Crítico, Alto y Medio):

Se analiza las vulnerabilidades del host mediante la herramienta de escaneo Nessus:

Figura 12. Información del Host zr03tc01.

Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 3

El host zr03tc01 presenta tres vulnerabilidades de alto grado de impacto, como se muestra en la tabla 16. Severidad critica del host zr03tc01.

Tabla 16. Severidad Crítica del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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	108797	Unsupported Windows OS

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de paquetes por parte del paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados a un servidor Windows.

  Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje vertificateVerify. Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente para el que no se ha solicitado un mensaje CertificateRequest.

- El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

  En Microsoft Server Message Block 1.0 (SMBv1) existen múltiples vulnerabilidades de ejecución de código remoto debido al tratamiento inadecuado de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades a través de un paquete especialmente diseñado, para ejecutar código arbitrario.

  Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través

de un paquete especialmente diseñado, para revelar información confidencial.

- El sistema operativo remoto o service pack ya no es compatible.

  A la versión remota de Microsoft Windows le falta un Service Pack o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Vulnerabilidad de Severidad Alta: 1

El host zr03tc01 presenta una vulnerabilidad que requiere atención de inmediata, como se muestra en la tabla 17. Severidad Alta del host zr03tc01.
Tabla 17. Severidad Alta del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Fuente: Propiedad del Autor.

- El host remoto de Windows podría permitir la ejecución arbitraria de código.

  Existe una vulnerabilidad arbitraria de código remoto en la implementación del Protocolo de Escritorio Remoto (RDP) en el directorio host Windows remoto. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en memoria que ha sido se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta opción para hacer que el sistema ejecute código arbitrario enviando una secuencia de RDP especialmente diseñada paquetes a él. Este plugin también comprueba si existe una vulnerabilidad de denegación de servicio en Microsoft Terminal Server. Tenga en cuenta que este script no detecta la vulnerabilidad si la opción Permitir conexiones sólo desde equipos que se ejecutan la configuración de "Escritorio remoto con autenticación a nivel de red" está activada o la capa de seguridad está establecida en "SSL (TLS 1.0)' en el host remoto.

Vulnerabilidad de Severidad Media: 9

El host zr03tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 18. Severidad media del host zr03tc01

Tabla 18. Severidad Media del host zr03tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad, (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC).
  Un ataque man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- Puede ser posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-themiddle (MiTM) . El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.
  Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a las colisiones ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado.
  Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017.

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se recomienda la encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

  La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

- El Terminal Services remoto no utiliza únicamente autenticación a nivel de red.

  El Terminal Services remoto no está configurado para utilizar únicamente autenticación a nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para llevar a cabo la autenticación de servidores mediante mecanismos TLS/SSL o Kerberos, que protegen contra los ataques del tipo "man-in-the-middle". Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios y software maliciosos al completar la autenticación de usuario antes de que se establezca una conexión RDP completa.

- El host remoto está usando criptografía débil.

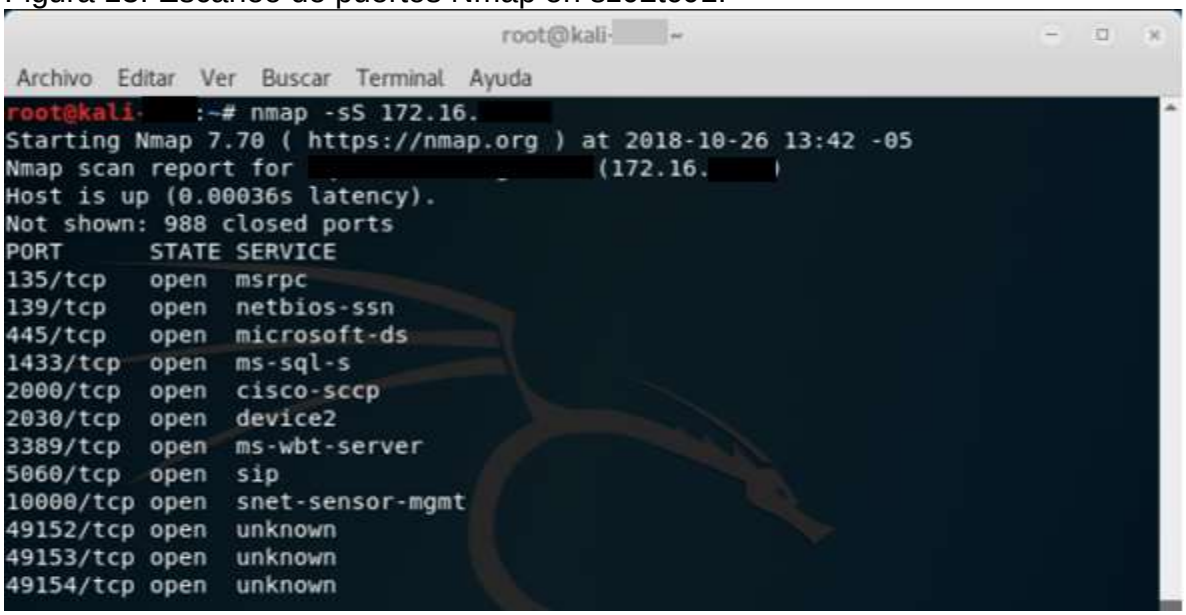
  El uso de criptografía débil con este servicio puede permitir que un atacante escuche las comunicaciones más fácilmente y obtenga capturas de pantalla y/o pulsaciones de teclas.

6.6.7 Repositorio Base de Datos SICA Host: sz02tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, son de estados desconocidos como se muestra en la figura 13. Escaneo de puertos Nmap en sz02tc01.

Figura 13. Escaneo de puertos Nmap en sz02tc01.



Fuente: Propiedad del Autor.

Analiza los reportes del escaneo de vulnerabilidades con la herramienta Nessus, Se analiza los reportes del escaneo de vulnerabilidades, detallando la información del host y cada vulnerabilidad teniendo en cuenta la información según el nivel de severidad (nivel Crítico, Alto y Medio) producto de los reportes de la herramienta Nessus:

Figura 14. Información del Host sz02tc01.

Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 2.

El host sz02tc01 presenta dos vulnerabilidades de alto grado de impacto, como se muestra en la tabla 19. Severidad critica del host sz02tc01.

Tabla 19. Severidad Crítica del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (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)

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto.

  El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto debido a un procesamiento inadecuado de por el paquete de seguridad Secure Channel (Schannel). Un atacante puede explotar este problema enviando paquetes especialmente diseñados para un servidor Windows. Tenga en cuenta que este plugin envía un mensaje de enlace TLS de certificado de cliente seguido de un mensaje de CertificateVerify.

- El host Windows remoto se ve afectado por las siguientes vulnerabilidades:

  En Microsoft Server Message Block 1.0 (SMBv1) existen múltiples vulnerabilidades de ejecución de código remoto debido al tratamiento inadecuado de determinadas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.
  Existe una vulnerabilidad de revelación de información en Microsoft Server Message Block 1.0 (SMBv1) debido en la tramitación de determinadas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial.

Vulnerabilidad de Severidad Alta: 2.

El host sz02tc01 presenta dos vulnerabilidades que requiere atención de inmediata, como se muestra en la tabla 20. Severidad Alta del host sz02tc01.

Tabla 20. Severidad Alta del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	N/A	20007	SSL Version 2 and 3 Protocol Detection

Fuente: Propiedad del Autor.

- El host remoto de Windows podría permitir la ejecución arbitraria de código.

  Existe una vulnerabilidad arbitraria de código remoto en la implementación del Protocolo de Escritorio Remoto (RDP) en el directorio host Windows remoto. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en memoria que ha sido se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta opción. Para hacer que el sistema ejecute código arbitrario enviando una secuencia de RDP especialmente diseñada de paquetes. Este plugin también comprueba si existe una vulnerabilidad de denegación de servicio en Microsoft Terminal Server.

- El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas. El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectado por varios defectos criptográficos:

  Planes inseguros de renegociación y reanudación de las sesiones. Un atacante puede explotar estas fallas para realizar ataques de hombre en el medio o para descifrar comunicaciones entre el servicio y los clientes afectados.
  Aunque SSL/TLS tiene un medio seguro para elegir la versión más alta soportada del protocolo (de modo que estas versiones sólo se utilizarán si el cliente o el servidor no soportan nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE).

Vulnerabilidad de Severidad Media: 11.

El host sz02tc01 presenta seis vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 21. Severidad media del host sz02tc01.

Tabla 21. Severidad Media del host sz02tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el Administrador de cuentas de seguridad. (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación por procedimiento Remoto (RPC). Un atacante man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos SAM, pueden explotar esto para forzar el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- Es posible obtener acceso al host remoto.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques man-in-themiddle (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar encriptación.
  Un atacante con la capacidad de interceptar tráfico desde el servidor RDP, puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.
  Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a este tipo de ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite a un atacante para que se haga pasar por el servicio afectado.

- El certificado SSL para este servicio es para un host diferente.

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

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.
  El host remoto soporta el uso de cifrados SSL con cifrado de fuerza media. Se considera de cambiar las longitudes de clave de al menos 64 bits o de 112 bits, o bien que utilice la suite de encriptación 3DES.

- La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

- Es posible obtener información sensible del host remoto con servicios habilitados para SSL/TLS.

  El host remoto se ve afectado por una vulnerabilidad de revelación de información de hombre en el medio (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar los mensajes.

- Fue posible obtener información sensible del host remoto con los servicios habilitados para TLS.

  El host remoto se ve afectado por una vulnerabilidad de revelación de información de hombre en el medio (MitM) conocida como POODLE. La vulnerabilidad se debe a que el servidor TLS no verifica el relleno de cifrado por bloques cuando utiliza un conjunto de como AES y DES. La falta de comprobación de relleno puede permitir descifrar el tráfico TLS cifrado. Esta vulnerabilidad podría permitir el descifrado del tráfico HTTPS por un tercero no autorizado.

- El host remoto está usando criptografía débil.

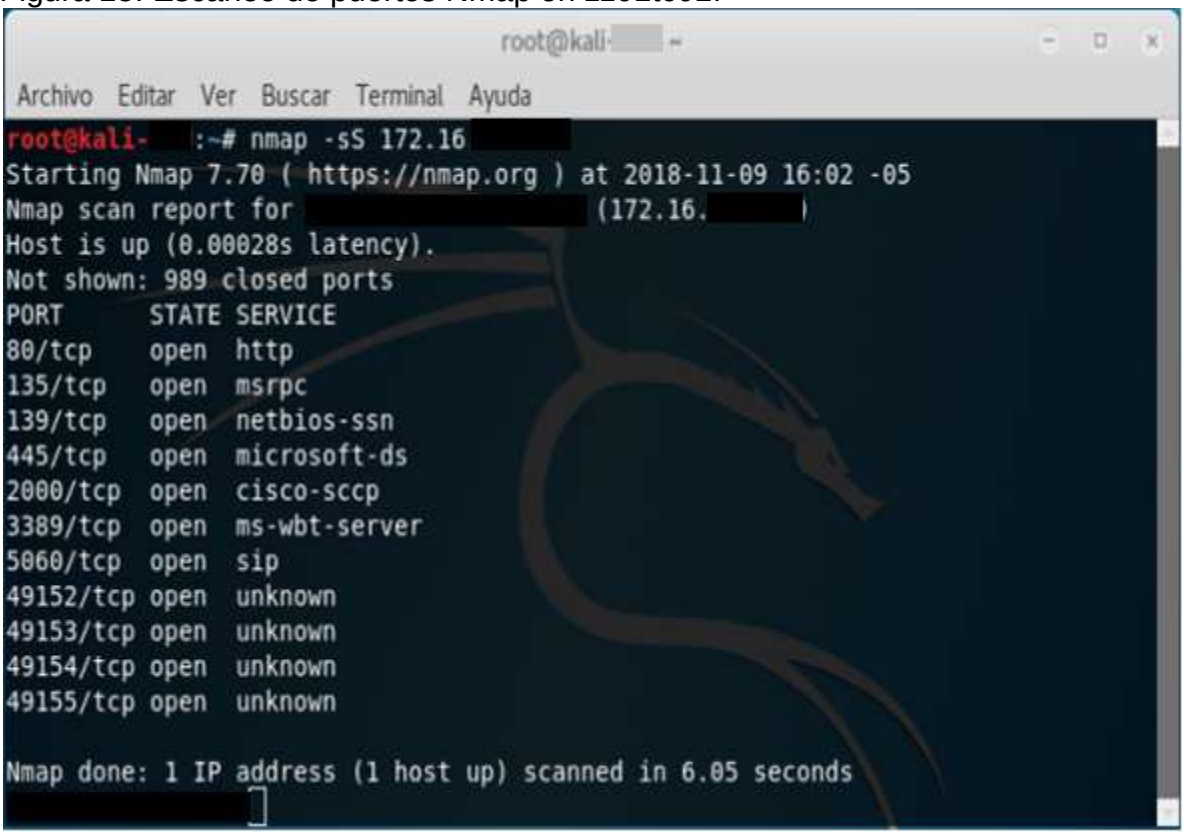
  El servicio de Terminal Services remoto no está configurado para utilizar criptografía fuerte. El uso de criptografía débil con este servicio puede permitir a un atacante espiar las comunicaciones y obtener capturas de pantalla y/o pulsaciones de teclas.

6.6.8 Producción Jones Host: zz01tc01 IP: 172.16.X.X

A continuación se realiza el escaneo, reconocimiento y enumeración de los servicios.

En los puertos de servicios, se evidencia que los puerto 49152/TCP, 49153/TCP, 49154/TCP, 49155/TCP, son de estados desconocidos como se muestra en la figura 15. Escaneo de puertos Nmap en zz01tc01.

Figura 15. Escaneo de puertos Nmap en zz01tc01.



Fuente: Propiedad del Autor.

Se analiza las vulnerabilidades del host mediante la herramienta de escaneo Nessus:

Analiza los reportes del escaneo de vulnerabilidades con la herramienta Nessus, detallando la información del host y cada vulnerabilidad teniendo en cuenta las vulnerabilidades según el nivel de severidad (nivel Crítico, Alto y Medio):

Figura 16. Información del Host zz01tc01.

Fuente: Propiedad del Autor.

Vulnerabilidad de Severidad Crítica: 1.

El host zz01tc01 presenta una vulnerabilidad de alto grado de impacto, como se muestra en la tabla 22. Severidad critica del host zz01tc01.

Tabla 22. Severidad Crítica del host zz01tc01

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en la pila de protocolos HTTP.

  La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de números enteros en la pila de protocolos HTTP (HTTP.sys) debido a un análisis inadecuado de las solicitudes HTTP creadas. Un dispositivo remoto no autenticado puede explotar esto para ejecutar código arbitrario con privilegios de Sistema.

Vulnerabilidad de Severidad Alta: 0.

- En el Host zz01tc01 no se encontró ninguna severidad crítica que pueda comprometer el host.

Vulnerabilidad de Severidad Media: 9.

El host zz01tc01 presenta nueve vulnerabilidades que requiere atención de tipo estándar, como se muestra en la tabla 23. Severidad media del host zz01tc01
Tabla 23. Severidad Media del host zz01tc01.

SEVERITY	CVSS	PLUGIN	NAME
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	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Fuente: Propiedad del Autor.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

El host remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en el administrador cuentas de seguridad (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a un nivel de autenticación inadecuado de negociación sobre los canales de Llamada de Procedimiento Remoto (RPC). Un ataque man-in-the-middle es capaz de interceptar las comunicaciones entre un cliente y un servidor que alberga una base de datos explotando y forzando el nivel de autenticación a downgrade, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la función Base de datos SAM.

- El host Windows remoto se ve afectado por una elevación de la vulnerabilidad de privilegios.

  La versión remota de Remote Desktop Protocol Server (Terminal Service) es vulnerable a los ataques de man-in-themiddle (MiTM) el cliente RDP no realiza la validación de la identidad del servidor mediante encriptación. Un atacante con la capacidad de interceptar tráfico desde el servidor RDP puede establecer encriptación con la directiva cliente y servidor sin ser detectados. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier la información confidencial transmitida, incluidas las credenciales de autenticación.
  Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Cualquier El usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y utilizarla para este ataque.

- No es necesario firmar en el servidor SMB remoto.

  No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovecharse de esto para realizar ataques man-in-the-middle contra el servidor SMB.

- Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.

  El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un hashing criptográficamente débil. (Por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a las colisiones ataques. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que permite una atacante para que se haga pasar por el servicio afectado. Tenga en cuenta que este plugin informa de todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017.

- El servicio remoto soporta el uso de cifrado SSL de nivel medio.

  El host remoto soporta el uso de cifrados SSL que ofrecen cifrado de fuerza media. Se recomienda la encriptación que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice la suite de encriptación ADES.

- El Terminal Services remoto no utiliza únicamente autenticación a nivel de red.

  El Terminal Services remoto no está configurado para utilizar únicamente autenticación a nivel de red (NLA). NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para llevar a cabo la autenticación de servidores mediante mecanismos TLS/SSL o Kerberos, que protegen contra los ataques del tipo "man-in-the-middle". Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios y software maliciosos al completar la autenticación de usuario antes de que se establezca una conexión RDP completa.

6.7 PRESENTACIÓN DE LOS SERVICIOS QUE SE IMPLEMENTARA EN LA ORGANIZACIÓN CASO DE ESTUDIO, DETALLANDO LA EJECUCIÓN.

Se describen las respectivas recomendaciones para los Host críticos (servidores y máquinas virtuales):

6.7.1 Publiquemos 1 Host: oa11tc01 IP: 172.16.X.X

Severidad Crítica.

Actualice a una versión de Oracle WebLogic más actual.

Severidad Alta.

Aplicar el parche de acuerdo con la última actualización de parches críticos de Oracle lanzado en el mes de julio de 2018.

Severidad Media.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

6.7.2 Publiquemos 2 Host: oa02tc01 IP: 172.16.X.X

Severidad Crítica.

Actualice a una versión de Oracle WebLogic más actual.

Severidad Alta.

Aplicar el parche de acuerdo con la última actualización de parches críticos de Oracle lanzado en el mes de julio de 2018.

Severidad Media.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

6.7.3 Aplicaciones Kactus Host: pt41tc01 IP: 172.16.X.X

Severidad Crítica.

Microsoft ha lanzado un conjunto de parches para Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 y 2012 R2.

Severidad Alta.

Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.1 (con suites de cifrado aprobadas) o superior en su lugar.

Severidad Media.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Genere y vuelva a emitir un nuevo certificado SSL para reemplazar el existente.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

6.7.4 Producción Base de Datos Host: zw03tc01 IP: 172.16.X.X

Severidad Crítica.

Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

Severidad Alta.

Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

Severidad Media.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red'. si está disponible.

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

Generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

6.7.5 Morfeus Host: zy03tc01 IP: 172.16.X.X

Severidad Crítica.

Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

Severidad Alta.

Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

Severidad Media.

Consulte la documentación del producto para eliminar las cifras débiles.

Genere un nuevo certificado SSL para reemplazar el existente.

Póngase en contacto con la Autoridad de Certificación para que se vuelva a emitir un nuevo certificado.

Adquirir o generar un certificado adecuado para este servicio.

6.7.6 Servidor de Aplicaciones SICA Host: zr03tc01 IP: 172.16.X.X

Severidad Crítica.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, y 2016. Microsoft también ha lanzado parches de seguridad para los sistemas operativos Windows que ya no son necesarios, soportado, incluyendo Windows XP, 2003, y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda a los usuarios que dejen de utilizar el uso de SMBv1. SMBv1 carece de las características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede desactivarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB

Severidad Alta.

Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Se debe Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.

Severidad Media.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red' si está disponible.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Póngase en contacto con la Autoridad de Certificación para que se vuelva a emitir el certificado.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

Adquirir o generar un certificado adecuado para este servicio.

Habilite la autenticación a nivel de red (NLA) en el servidor RDP remoto. Esto se realiza generalmente en la pestaña "Remoto" de la configuración "Sistema" de Windows.

Cambie el nivel de cifrado RDP a uno de:
3. High
4. FIPS Compliant

6.7.7 Repositorio Base de datos SICA Host: sz02tc01 IP: 172.16.X.X

Severidad Crítica.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluyendo Windows XP, 2003 y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 carece de las funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1.

Severidad Alta.

Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Se debe Tener en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.

Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.1 (con suites de cifrado aprobadas) o superior en su lugar.

Severidad Media.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o Seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red'.

Imponga la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de claves de nivel medio.

Desactivar SSLv3. Los servicios que deben ser compatibles con SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda utilizar SSLv3.

Actualizar parches de seguridad

Cambie el nivel de cifrado RDP a uno de:
3. High
4. FIPS Compliant

6.7.8 Producción Jones Host: zz01tc01 IP: 172.16.X.X

Severidad Crítica.

Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2. Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 porque carece de las funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1.

Severidad Alta.

No necesita soluciones

Severidad Media.

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, o/y seleccionar la opción `Permitir conexiones sólo desde ordenadores que ejecuten escritorio remoto con autenticación a nivel de red'.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

Habilite la autenticación a nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña "Remoto" de la configuración "Sistema" de Windows.

RECOMENDACIONES

Se describen las respectivas recomendaciones para los Host críticos (servidores y máquinas virtuales):

- **Publiquemos 1 Host:oa11tc01 IP: 172.16.X.X**

  Severidad Crítica

  Actualice a una versión de Oracle WebLogic más actual.

  Severidad Alta

  Aplicar el parche de acuerdo con la última actualización de parches críticos de Oracle lanzado en el mes de julio de 2018.

  Severidad Media

  Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

  Adquirir o generar un certificado adecuado para este servicio.

- **Publiquemos 2 Host: oa02tc01 IP: 172.16.X.X**

  Severidad Crítica

  Actualice a una versión de Oracle WebLogic más actual.

  Severidad Alta

  Aplicar el parche de acuerdo con la última actualización de parches críticos de Oracle lanzado en el mes de julio de 2018.

  Severidad Media

  Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

- **Aplicaciones Kactus Host: pt41tc01 IP: 172.16.X.X**

  Severidad Crítica

  Microsoft ha lanzado un conjunto de parches para Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 y 2012 R2.

  Severidad Alta

  Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.1 (con suites de cifrado aprobadas) o superior en su lugar.

  Severidad Media

  Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

  Genere y vuelva a emitir un nuevo certificado SSL para reemplazar el existente.

  Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

- **Producción Base de Datos Host: zw03tc01 IP: 172.16.X.X**

  Severidad Crítica

  Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

  Severidad Alta

  Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

  Severidad Media

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red'. si está disponible.

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

Generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

- **Morfeus Host: zy03tc01 IP: 172.16.X.X**

  Severidad Crítica

  Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

  Severidad Alta

  Actualice a la versión 7.6 o posterior de la página principal de HP System Management (SMH).

  Severidad Media

  Consulte la documentación del producto para eliminar las cifras débiles.

  Genere un nuevo certificado SSL para reemplazar el existente.

  Póngase en contacto con la Autoridad de Certificación para que se vuelva a emitir un nuevo certificado.

  Adquirir o generar un certificado adecuado para este servicio.

- **Servidor de Aplicaciones SICA Host: zr03tc01 IP: 172.16.X.X**

  Severidad Crítica

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, y 2016. Microsoft también ha lanzado parches de seguridad para los sistemas operativos Windows que ya no son necesarios, soportado, incluyendo Windows XP, 2003, y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda a los usuarios que dejen de utilizar el uso de SMBv1. SMBv1 carece de las características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede desactivarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB

Severidad Alta

Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Se debe Tenga en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.

Severidad Media

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red' si está disponible.

Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Póngase en contacto con la Autoridad de Certificación para que se vuelva a emitir el certificado.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

Adquirir o generar un certificado adecuado para este servicio.

Habilite la autenticación a nivel de red (NLA) en el servidor RDP remoto. Esto se realiza generalmente en la pestaña "Remoto" de la configuración "Sistema" de Windows.

Cambie el nivel de cifrado RDP a uno de:
3. High
4. FIPS Compliant

- **Repositorio Base de datos SICA Host: sz02tc01 IP: 172.16.X.X**

  Severidad Crítica

  Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluyendo Windows XP, 2003 y 8.

  Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 carece de las funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1.

  Severidad Alta

  Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2. Se debe Tener en cuenta que se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows 2000.

  Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. Utilice TLS 1.1 (con suites de cifrado aprobadas) o superior en su lugar.

  Severidad Media

  Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

  Forzar el uso de SSL como capa de transporte para este servicio si es compatible, y/o Seleccione la opción 'Permitir conexiones sólo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red'.

  Imponga la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

Adquirir o generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de claves de nivel medio.

Desactivar SSLv3. Los servicios que deben ser compatibles con SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda utilizar SSLv3.

Actualizar parches de seguridad

Cambie el nivel de cifrado RDP a uno de:
3. High
4. FIPS Compliant

- **Producción Jones Host: zz01tc01 IP: 172.16.X.X**

  Severidad Crítica

  Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2. Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 porque carece de las funciones de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1.

  Severidad Alta

  No necesita soluciones

  Severidad Media

  Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

  Forzar el uso de SSL como capa de transporte para este servicio si es compatible, o/y seleccionar la opción `Permitir conexiones sólo desde ordenadores que ejecuten escritorio remoto con autenticación a nivel de red'.

  Imponga la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft': Firmar digitalmente las comunicaciones (siempre)". En Samba, la configuración se llama 'firma de servidor'.

  Adquirir o generar un certificado adecuado para este servicio.

Reconfigure la aplicación afectada si es posible para evitar el uso de cifras de fuerza media.

Habilite la autenticación a nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña "Remoto" de la configuración "Sistema" de Windows.

CONCLUSIONES

- Al realizar la recolección de información se determinaron y se seleccionaron los host más críticos teniendo en cuenta que son servicios que se en cuenta expuestos, por los cuales se desarrolló el análisis de vulnerabilidades, permitiendo la categorización y clasificación según su severidad.

- Frente a las evidencias recaudadas en la organización caso de estudio, la severidad con mayor índice es la de nivel alto, ya que estas vulnerabilidades presentan características que ponen en peligro la seguridad, confidencialidad e integridad de la información.

- Dentro de los análisis expuestos de vulnerabilidades, fue posible identificar cuáles son las vulnerabilidades más críticas que pueden generar riesgo a la seguridad de la organización caso de estudio.

- Al efectuar el análisis de vulnerabilidades a través de la metodología "PenTest" con el software Nesuss, se evidencio que los host presentan falta de actualizaciones de parches de seguridad de Windows y certificaciones que pueden poner en riesgo la información de la organización.

- Al reconocer las vulnerabilidades de cada uno de los host más críticos (servidores y máquinas virtuales) de infraestructura tecnológica de una forma ordenada, se entrega el debido informe del proceso, suministrado a la organización la comprensión del estado actual en materia de seguridad de la información, lo que permitirá a las directivas la toma de decisiones acertadas de mitigación de las vulnerabilidades encontradas

BIBLIOGRAFIA

CASTRO BOLAÑOS, Duvan. ROJAS MORA, Ángela. Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (Octubre 17 de 2012). Diario Oficial 48.587 de octubre 17 de 2012. p. 1-16.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341. Bogotá. (Julio 30 de 2009). Diario Oficial 47.426 de julio 30 de 2009. p. 1-10.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (Enero 5 de 2009). Diario Oficial 47.223 de enero 5 de 2008. p. 1-3.

CODIGO PROGRAMACION. Herramientas básicas para hacking (Escaneo). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://codigoprogramacion.com/tag/nmap-hacking#.XBPM54tKiUk

DESENREDADOS. Evaluación de amenaza, vulnerabilidad y el riesgo. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nmap.org/

FRANCO, David A. PEREA, Jorge L. PUELLO, Plinio, Metodología para la detección de vulnerabilidades en redes de datos. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://bibliotecavirtual.unad.edu.co:2139/eds/pdfviewer/pdfviewer?vid=1&sid=8cd37457-4010-4308-a0ad-b3b98f16c321%40pdc-v-sessmgr03

GARZÓN, Daniel. RATKOVICH GOMES, JUAN. Metodología de Análisis de Vulnerabilidades para Empresa de mediana y pequeña escala [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

GGI LAN GUARD 12. Vulnerabilidades y exposiciones comunes (CVE). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm

GUTIERREZ DE MORAL, Leonardo. Curso de ciberseguridad y hacking ético 2013, pág. 66. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=sua0BAAAQBAJ&lpg=PA66&dq=metodologia%20pentest&pg=PA67#v=onepage&q=metodologia%20pentest&f=false

INCIBE. Amenaza vs vulnerabilidades. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INFORMÁTICA. Kali Linux: Una distribución Linux especializada. [2018] [en línea] [citado el 13 de diciembre, 2018] Disponible en internet: https://inforseguridad.wordpress.com/2016/11/09/kali-linux-que-es-para-que-se-utiliza-las-diez-aplicaciones-mas-importantes-que-integra/

ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27001.] [Citado el 08 de noviembre, 2018] Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

KALI. Kali Linux. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.kali.org/

MEDINA, Javier, Evaluación de vulnerabilidades TIC, [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=GSuZBgAAQBAJ&lpg=PA22&dq=pruebas%20de%20vulnerabilidades

MOYANO ORJUELA, Luz. SUAREZ CÁRDENAS, Yasmin. Plan de Implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones. [2018] [en línea] [citado el 12 de diciembre ,2018] Disponible en internet: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

NMAP. Nmap. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nmap.org/man/es/index.html

NULLPROGRAM. The Arcfour Stream Cipher.). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nullprogram.com/blog/2008/08/09/

REVIVERSOFT. Nessus extension del archivo. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.reviversoft.com/es/file-extensions/nessus.

SECURITY HACKLABS. El sistema de detección de versiones de Nmap. [2018] [en línea] [citado el 12 de diciembre, 2018] Disponible en internet: https://securityhacklabs.net/articulo/el-sistema-de-deteccion-de-versiones-de-nmap

SYMANTEC CORPORATION. ¿En qué consiste el malware?). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.websecurity.symantec.com/es/es/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

UNIVERSIDAD DE CARTAGENA, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA. Metodología para la detección de Vulnerabilidades en Redes de Datos. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

UNIVERSIDAD NACIONAL DE LUJAN. Amenazas a la Seguridad de la Información. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

RESUMEN ANALITICO EN EDUCACIÓN – RAE

Información General	
1. Título	Análisis de vulnerabilidades de la infraestructura tecnológica de organización caso de estudio
2. Autor	Mario Andres Carvajal Avila
3. Edición	Universidad Nacional Abierta y a Distancia - UNAD
4. Fecha	12 de mayo del 2019
5. Palabras clave	Nmap, Kali Linux, Nessus, Host, Vulnerabilidades, Severidades, CVE, Exploit, mitigación, malware

6. Descripción.
El presente proyecto aplicativo tiene como finalidad explorar y aplicar las pruebas de vulnerabilidades mediante la utilización de herramientas, procesos y metodología de pruebas de vulnerabilidades. Se ha querido revisar y explorar las vulnerabilidades presentes en los host más críticos (servidores Físicos y máquinas virtuales) de la organización, con el fin de mitigar, solucionar, beneficiar y optimizar los recursos en los procesos que ejecuta la organización, manteniendo confidencialidad y seguridad de la información. En la organización caso de estudio se ha evidenciado ataques e intentos de accesos no autorizados, que han sido validados mediante herramientas de seguridad perimetral como el firewall, Analyzer y Sandbox, motivo por el cual es necesario aplicar el plan de pruebas y mitigación de vulnerabilidades sobre los hosts más críticos (servidores y máquinas virtuales) perteneciente a la organización caso de estudio. Para el desarrollo de la práctica se realizará mediante pruebas utilizadas de manera ordenada con la metodología de Ética Hacking para describir el proceso del desarrollo del proceso del plan de pruebas y mitigación de vulnerabilidades, además se manipulará herramientas de pen test y análisis que serán necesarios para realizar el procedimiento, así como Kali Linux, Nmap, Nessus. Los resultados del procedimiento en aplicar el escaneo y análisis de vulnerabilidades en la organización se detallara mediante un informe área de tecnología y cómputo de la organización caso de estudio la lista de las vulnerabilidades encontradas y certificadas mediante CVE (Common Vulnerabilities and Exposures), adicionalmente este documento se proporcionará una lista de recomendaciones que se deben aplicar e informando los resultados obtenidos antes y después, con el propósito de mitigar con soluciones que han sido detallados con las personas involucradas en área de tecnología y cómputo y aplicativos que operan los host más críticos de la organización caso estudio.

7. Fuentes.

25 Referencias Bibliográficas. Ejemplos de la bibliografía (15):

[1] CASTRO BOLAÑOS, Duvan. ROJAS MORA, Ángela. Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

[2] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

[3] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (Octubre 17 de 2012). Diario Oficial 48.587 de octubre 17 de 2012. p. 1-16.

[4] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341. Bogotá. (Julio 30 de 2009). Diario Oficial 47.426 de julio 30 de 2009. p. 1-10.

[5] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (Enero 5 de 2009). Diario Oficial 47.223 de enero 5 de 2008. p. 1-3.

[6] CODIGO PROGRAMACION. Herramientas básicas para hacking (Escaneo). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://codigoprogramacion.com/tag/nmap-hacking#.XBPM54tKiUk

[7] DESENREDADOS. Evaluación de amenaza, vulnerabilidad y el riesgo. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nmap.org/

[8] FRANCO, David A. PEREA, Jorge L. PUELLO, Plinio, Metodología para la detección de vulnerabilidades en redes de datos. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: http://bibliotecavirtual.unad.edu.co:2139/eds/pdfviewer/pdfviewer?vid=1&sid=8cd37457-4010-4308-a0ad-b3b98f16c321%40pdc-v-sessmgr03

[9] GARZÓN, Daniel. RATKOVICH GOMES, JUAN. Metodología de Análisis de Vulnerabilidades para Empresa de mediana y pequeña escala [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

[11] GGI LAN GUARD 12. Vulnerabilidades y exposiciones comunes (CVE). [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.html

[12] GUTIERREZ DE MORAL, Leonardo. Curso de ciberseguridad y hacking ético 2013, pág. 66. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://books.google.com.co/books?id=sua0BAAAQBAJ&lpg=PA66&dq=metodologia%20pentest&pg=PA67#v=onepage&q=metodologia%20pentest&f=false

[13] INCIBE. Amenaza vs vulnerabilidades. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[14] INFORMÁTICA. Kali Linux: Una distribución Linux especializada. [2018] [en línea] [citado el 13 de diciembre, 2018] Disponible en internet: https://inforseguridad.wordpress.com/2016/11/09/kali-linux-que-es-para-que-se-utiliza-las-diez-aplicaciones-mas-importantes-que-integra/

[15] NMAP. Nmap. [2018] [en línea] [citado el 08 de noviembre, 2018] Disponible en internet: https://nmap.org/man/es/index.html

8. Contenidos.

La información y los sistemas de las organizaciones son víctima de ataques que pueden ocurrir sobre aplicaciones o servicios expuestos, y otros son aprovechados por vulnerabilidades que se presenta en dichos sistemas.

"De este modo comienza con la planeación, la cual se encarga de valorar, analizar, y proyectar los di referentes riesgos que se encuentre presente en el ambiente empresarial. De acuerdo con este plan, se debe implementar políticas de seguridad, identificando las amenazas internas y externas, teniendo en cuenta la infraestructura tecnológica que posee. Luego se implementa la parte práctica, eligiendo y estableciendo arquitectura de red, en el cual se monte todos los servicios que presta la organización, asegurando cada uno de esto; llevando a cabo una auditoria de este proceso, la cual se debe seguir realizándose periódicamente"

Se hace necesario realizar un análisis de vulnerabilidades para identificar aquellas brechas de seguridad a las que se encuentran expuestas tanto externa e internamente la Institución. Este análisis de vulnerabilidades se realizará mediante escaneo de puertos activos y vulnerabilidades, en donde se aplican pruebas de "pen test" que son realizadas mediante metodologías de hacking ético con el uso de software y herramientas que son primordiales para este tipo de procedimiento.

Por lo tanto " Existen metodología la cual da a conocer una seria de pasos, que abracan diferentes temas como lo son la planeación, políticas de seguridad, aseguramiento de la seguridad de la información, haciendo que un sistema

permanezca cubierto y preparado ante eventualidad que puedan interrumpir el desarrollo normal de las actividades de una organización"

Con el análisis se logrará disminuir y controlar los peligros existentes a los que se encuentran expuestos los host más críticos de la Organización caso de estudio, así como también conocer la situación actual de seguridad de la organización con el fin de implementar medidas preventivas y correctivas con el fin mitigar dichos riesgos y amenazas.

9. Metodología.

Metodología de investigación aplicada, recolección, escaneo, procesamiento y análisis de datos de forma cualitativa y cuantitativa.

10. Conclusiones.

- Al realizar la recolección de información se determinaron y se seleccionaron los hosts más críticos teniendo en cuenta que son servicios que se en cuenta expuestos, por los cuales se desarrolló el análisis de vulnerabilidades, permitiendo la categorización y clasificación según su severidad.
- Frente a las evidencias recaudadas en la organización caso de estudio, la severidad con mayor índice es la de nivel alto, ya que estas vulnerabilidades presentan características que ponen en peligro la seguridad, confidencialidad e integridad de la información.
- Dentro de los análisis expuestos de vulnerabilidades, fue posible identificar cuáles son las vulnerabilidades más críticas que pueden generar riesgo a la seguridad de la organización caso de estudio.
- Al efectuar el análisis de vulnerabilidades a través de la metodología "PenTest" con el software Nesuss, se evidencio que los host presentan falta de actualizaciones de parches de seguridad de Windows y certificaciones que pueden poner en riesgo la información de la organización.
- Al reconocer las vulnerabilidades de cada uno de los host más críticos (servidores y máquinas virtuales) de infraestructura tecnológica de una forma ordenada, se entrega el debido informe del proceso, suministrado a la organización la comprensión del estado actual en materia de seguridad de la información, lo que permitirá a las directivas la toma de decisiones acertadas de mitigación de las vulnerabilidades encontradas

11. Autor del RAE.

Mario Andrés Carvajal Avila