

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

ANÁLISIS DE SEGURIDAD INFORMÁTICA SOBRE EL IMPACTO DE LAS VULNERABILIDADES EN LOS SERVIDORES INTERNOS DE EMAPA

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

ÁREA: Seguridad de redes

LÍNEA DE INVESTIGACIÓN: Tecnología de la información y Sistemas de control

AUTOR: Andrés Steven Carrera Aguaguiña

TUTOR: Ing. David Omar Guevara Aulestia Mg.

Ambato - Ecuador

julio – 2025

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: ANÁLISIS DE SEGURIDAD INFORMÁTICA SOBRE EL IMPACTO DE LAS VULNERABILIDADES EN LOS SERVIDORES INTERNOS DE EMAPA, desarrollado bajo la modalidad Proyecto de Investigación por el señor Andrés Steven Carrera Aguaguiña, estudiante de la Carrera de Ingeniería en Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, julio 2025.

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA
Validar únicamente con FirmaEC

Ing. David Omar Guevara Aulestia, Mg.
TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: ANÁLISIS DE SEGURIDAD INFORMÁTICA SOBRE EL IMPACTO DE LAS VULNERABILIDADES EN LOS SERVIDORES INTERNOS DE EMAPA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio 2025.



Andrés Steven Carrera Aguaguiña

C.C. 185021571-4

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, julio 2025.



Andrés Steven Carrera Aguaguiña

C.C. 1850215714

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Andrés Steven Carrera Aguaguiña, estudiante de la Carrera en Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado ANÁLISIS DE SEGURIDAD INFORMÁTICA SOBRE EL IMPACTO DE LAS VULNERABILIDADES EN LOS SERVIDORES INTERNOS DE EMAPA nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, julio 2025.

Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA
Validar únicamente con FirmaEC

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
DANIEL SEBASTIAN JEREZ MAYORGA
Validar únicamente con FirmaEC

Ing. Daniel Jerez Mayorga, MSc.
PROFESOR CALIFICADO

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA
Validar únicamente con FirmaEC

Ing. Vicente Morales Lozada, Mg
PROFESOR CALIFICADOR

DEDICATORIA

A Dios, por haber sido mi guía, mi fortaleza y mi luz en cada paso de este camino. Sin su sabiduría y dirección, este logro no habría sido posible. También a mis padres, por su amor incondicional, sacrificio constante apoyo en todo momento. Gracias por creer en mí, por motivarme a seguir adelante y por ser el pilar fundamental de mi vida.

A los ingenieros y docentes que, a lo largo de mi formación académica, compartieron sus conocimientos, ofrecieron su guía y me impulsaron a superarme. Cada enseñanza recibida fue una herramienta valiosa en la construcción de este proyecto.

AGRADECIMIENTO

Agradezco primeramente a Dios, por brindarme la vida, la salud y la sabiduría necesaria para alcanzar esta meta. Su presencia ha sido mi mayor sostén en los momentos de incertidumbre, y Su guía me ha permitido superar cada obstáculo con fe y perseverancia.

A mis padres, por su amor incondicional, apoyo constante y sacrificios diarios. Gracias por ser mi inspiración y por enseñarme, con el ejemplo, el valor del esfuerzo y la dedicación.

A mis docentes e ingenieros que me acompañaron a lo largo de la carrera, por compartir sus conocimientos, por sus enseñanzas y por motivarme a crecer tanto profesional como personalmente. Su guía ha sido clave en mi formación.

A mis compañeros, amigos y todas las personas que de alguna manera fueron parte de este proceso, les extiendo mi sincero agradecimiento por su apoyo, colaboración y palabras de aliento.

Este logro es el resultado de un camino recorrido con esfuerzo, constancia y el respaldo de todos ustedes.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA ..... **i**

APROBACIÓN DEL TUTOR ..... **ii**

AUTORÍA ..... **iii**

DERECHOS DE AUTOR ..... **iv**

APROBACIÓN DEL TRIBUNAL DE GRADO ..... **v**

DEDICATORIA ..... **vi**

AGRADECIMIENTO ..... **vii**

ÍNDICE GENERAL DE CONTENIDOS ..... **viii**

ÍNDICE DE TABLAS ..... **xii**

ÍNDICE DE FIGURAS ..... **xiii**

ÍNDICE DE ANEXOS ..... **xvii**

RESUMEN EJECUTIVO ..... **xviii**

ABSTRACT ..... **xix**

CAPÍTULO I. MARCO TEÓRICO **1**

1.1 Tema de investigación 1

1.1.1 Planteamiento del problema 1

1.2 Antecedentes investigativos 2

1.3 Fundamentación teórica 5

1.3.1 Tecnologías de las Información 5

1.3.2 Seguridades 6

1.3.3 Análisis de Servidores 6

1.3.4 Auditoría de Seguridad Informática 6

1.3.5 Seguridad de la Información 7

1.3.6 Automatización y Control de Servidores 7

1.3.7 Mitigación de Vulnerabilidades 8

1.3.8 Eficiencia Operativa 8

1.4 Objetivos 9

1.4.1 Objetivo general 9

1.4.2 Objetivos específicos 9

CAPÍTULO II. METODOLOGÍA 10

2.1 Materiales 10

2.2 Métodos 14

2.2.1 Modalidad de la investigación 15

2.2.2 Población y muestra 15

2.2.3 Recolección de información 16

2.2.4 Procesamiento y análisis de datos 31

CAPÍTULO III. RESULTADOS Y DISCUSIÓN 32

3.1 Análisis y discusión de los resultados 32

3.1.1 Aplicación de la Metodología WSP 32

3.2 Desarrollo de la propuesta 34

3.2.1 Levantamiento de activos tecnológicos 34

3.2.2 Selección de la herramienta de análisis de seguridad informática 37

3.2.3 Análisis de las vulnerabilidades en los servidores internos de EMAPA..... 39

3.2.3.1 Servidor 1 de Correo 39

3.2.3.2 Servidor 2 SGBD Documental 42

3.2.3.3 Servidor 3 Comercial 49

3.2.3.4 Servidor 4 BD Comercial 52

3.2.3.5 Servidor 5 Administrativo 54

3.2.3.6 Servidor 6 Dominio SSL EMAPA 62

3.2.3.7 Servidor 7 BD Administrativo EMAPA 67

3.2.3.8 Servidor 8 Servicios en línea EMAPA 69

3.2.3.9 Servidor 9 Dominio EMAPA 74

3.2.3.10 Servidor 10 Aplicaciones EMAPA 79

3.2.3.11 Servidor 11 Licencias WSCAD EMAPA 81

3.2.3.12 Servidor 12 Antivirus EMAPA 82

3.2.3.13 Servidor 13 Registros Asistencia EMAPA 88

3.2.3.14 Servidor 14 Desarrollo EMAPA 97

3.2.3.15 Servidor 15 Cliente GIS EMAPA 98

3.2.3.16 Servidor 16 Help Desk 100

3.2.3.17 Servidor 17 BD Servicios en Línea 101

3.2.3.18 Servidor 18 Financiero Antiguo 115

3.2.3.19 Servidor 19 Comercial 122

3.2.3.20 Servidor 20 Documental 130

3.3 Estadísticas de Criticidad de las herramientas Nessus, Nmap y OpenVas 139

3.4 Entrega del Informe a Jefatura de TI de la empresa EMAPA 146

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 147

4.1 Conclusiones 147

4.2 Recomendaciones 148

REFERENCIAS BIBLIOGRÁFICAS 149

ANEXOS 153

ÍNDICE DE TABLAS

Tabla 1. Cadenas de Búsqueda aplicadas en base de datos científicas 2

Tabla 2. Filtro de búsqueda aplicado en repositorio de universidades de Ecuador 3

Tabla 3. Criterios de Inclusión y Exclusión 3

Tabla 4. Ficha de Observación 14

Tabla 5. Población de estudio 16

Tabla 6. Cálculos de las Varianzas y Sumatorias 17

Tabla 7. Resutados estadisticos del coeficiente Alfa de Cronbach 17

Tabla 8. Interpretación de confiabilidad 17

Tabla 9. Resultados de la ficha de observación 29

Tabla 10. Levantamiento de activos servidores internos de EMAPA..... 34

ÍNDICE DE FIGURAS

Figura 1. Cargo que tiene el personal de TI 18

Figura 2. Identificación de los años de experiencia del personal de TI 19

Figura 3. Frecuencia de los análisis de seguridad en los servidores internos 20

Figura 4. Herramientas de la detección de vuleabilidades 20

Figura 5. Capacitación informática y gestión de vulnerabilidades 21

Figura 6. Corrección de las vulnerabiliades en EMAPA 22

Figura 7. Acciones o prácticas que se aplican para proteger los servidores internos 22

Figura 8. Priorización de las vulnerabilidades detectadas 23

Figura 9. Procesos que sean los más afectados contra una vulnerabilidad crítica 23

Figura 10. Servicios a fallos de seguridad informática 24

Figura 11. Impacto principal 25

Figura 12. Recursos suficientes para proteger los servidores internos de EMAPA . 25

Figura 13. Resultado escanéo Servidor 1 de Correo 39

Figura 14. Resultado Servidor 2 SGBD Documental 42

Figura 15. Resultado Servidor 3 Comercial 49

Figura 16. Resultado Servidor 4 BD Comercial 52

Figura 17. Resultado Servidor 5 Administrativo 54

Figura 18. Resultado Servidor 6 Dominicio SSL EMAPA 62

Figura 19. Resultado Servidor 7 BD Administrativo EMAPA 67

Figura 20. Resultado Servidor 8 Servicios en línea EMAPA 69

Figura 21. Resultado Servidor 9 Dominio EMAPA 74

Figura 22. Resultado Servidor 10 Aplicaciones Emapa 79

Figura 23. Resultado Servidor 11 Licencias WSCAD EMAPA..... 81

Figura 24. Resultado Servidor 12 Antivirus EMAPA 82

Figura 25. Resultado Servidor 13 Resgistros Asistencias EMAPA..... 88

Figura 26. Resultado Servidor 14 Desarrollo EMAPA..... 97

Figura 27. Resultado Servidor 15 Cliente GIS Emapa 98

Figura 28. Resultado Servidor 6 Help Desk 100

Figura 29. Resultado BD Servidor 17 Servicios en Línea 101

Figura 30. Resultado Servidor 18 Financiero Antiguo 115

Figura 31. Resultado Servidor 19 Comercial..... 122

Figura 32. Resultado Servidor 20 Documental..... 130

Figura 33. Matriz de riesgo de los 20 Servidores virtualizados..... 139

Figura 34. Criticidad media en Servidor 1 Correo con OpenVas 139

Figura 35. Criticidad media en Servidor 2 SGBD Documental con Nmap 140

Figura 36. Criticidad media en Servidor 3 Comercial EMAPA con Nmap..... 140

Figura 37. Criticidad baja en Servidor 4 BD Comercial EMAPA con OpenVas ... 140

Figura 38. Criticidad media en Servidor 5 Administrativo EMAPA con Nmap 141

Figura 39. Criticidad media en Servidor 6 Dominio con Nmap 141

Figura 40. Criticididad media en Servidor 7 BD Administrativo con Nmap 141

Figura 41. Criticidad alta en Servidor 8 Servicios en Línea EMAPA con Nmap... 142

Figura 42. Criticidad media en Servidor 9 Dominio con Nessus y OpenVas..... 142

Figura 43. Criticidad media en Servidor 10 Aplicaciones con Nessus..... 142

Figura 44. Criticidad media en Servidor 11 Licencias WSCAD con Nessus..... 143

Figura 45. Criticidad media en Servidor 12 Antivirus con Nessus..... 143

Figura 46. Criticidad alta y media en Servidor 13 Registro de asistencia con Nessus y OpenVas..... 143

Figura 47. Criticidad media en Servidor 14 Desarrollo con Nmap 144

Figura 48. Criticidad media en Servidor 15 Cliente GIS con Nmap 144

Figura 49. Criticidad alta y baja en Servidor 16 Help Desk con Nmap y OpenVas144

Figura 50. Criticidad alta y media en Servidor 17 BD Servicios en Línea con OpenVas..... 145

Figura 51. Criticidad media en Servidor 18 Financiero Antiguo con OpenVas..... 145

Figura 52. Criticidad media en Servidor 19 Comercial Antiguo con Nessus..... 145

Figura 53. Criticidad Servidor 20 Documental Antiguo..... 146

Figura 54. Portada del Informe de Vulnerabilidades Jefe de TI..... 146

Figura 55. Instalación AlmaLinux en la consola de AlmaLinux..... 153

Figura 56. Paquetes descargados desde Almalinux 153

Figura 57. Inicilización del servicio de Nessus 153

Figura 58. Ingreso con la IP de la herramienta Nessus en el navegador..... 154

Figura 59. Interfaz de la Inicialización de la herramienta de Nessus 154

Figura 60. Plataformas de bienvenida para aceptar el registro 154

Figura 61. Platafoma de registro en la herramienta de Nessus 155

Figura 62. Código de activación 155

Figura 63. Descarga de los plugins 156

Figura 64. Interfaz de Nessus para lo su utilidad 156

Figura 65. Configuración de la IP estática 156

Figura 66. Plantilla de Excel Matriz de Riesgo 157

Figura 67. Plantilla de Excel Resumen Estadístico 157

ÍNDICE DE ANEXOS

Anexo A. Instalación de Nessus en AlmaLinux 153

Anexo B. Plantilla Matriz de Riesgo 157

RESUMEN EJECUTIVO

Actualmente, las instituciones dependen fuertemente de la tecnología, lo que también las hace vulnerables a amenazas informáticas. En el caso de EMAPA, resulta fundamental proteger sus servidores internos para evitar afectaciones en la operatividad y seguridad de la información. Por esta razón, este proyecto tiene como objetivo analizar la seguridad informática en dichos servidores y detectar posibles vulnerabilidades que puedan comprometer su funcionamiento.

La investigación inició con un levantamiento de los activos tecnológicos, permitiendo conocer la infraestructura actual y los servicios críticos que soportan. Luego, se aplicó una metodología de tipo aplicada y descriptiva, evaluando distintas herramientas de análisis de vulnerabilidades utilizando Nessus, Nmap, y OpenVas en función de su precisión, facilidad de uso y efectividad. A partir de esta comparación, se eligió la herramienta más adecuada para ejecutar escaneos exhaustivos.

Los resultados obtenidos permitieron identificar vulnerabilidades clasificadas por niveles de criticidad, lo cual ayudó a medir el grado de exposición ante amenazas. En base a estos hallazgos, se propusieron medidas de remediación ajustadas a las capacidades de EMAPA. Estas recomendaciones tienen como propósito fortalecer la seguridad de los sistemas, prevenir incidentes y optimizar la gestión de riesgos tecnológicos.

Finalmente, el estudio resalta se debe controles periódicos de seguridad informática en lo servidores de la organización institucional proporciona información útil para la toma de decisiones técnicas y estratégicas en la protección de los activos digitales institucionales.

Palabras clave: Seguridad informática, vulnerabilidades, servidores, EMAPA, remediación.

ABSTRACT

Currently, institutions rely heavily on technology, which also makes them vulnerable to cybersecurity threats. In the case of EMAPA, it is essential to safeguard its internal servers to prevent disruptions in operations and to ensure the security of sensitive information. For this reason, the objective of this project is to analyze the cybersecurity posture of these servers and identify potential vulnerabilities that could compromise their functionality.

The research began with a thorough inventory of technological assets, providing a clear understanding of the current infrastructure and the critical services it supports. An applied and descriptive methodology was then employed, evaluating various vulnerability analysis tools namely Nessus, Nmap, and OpenVAS based on their accuracy, ease of use, and overall effectiveness. From this comparison, the most suitable tool was selected to carry out in-depth scans.

The results revealed vulnerabilities categorized by severity levels, which helped assess the organization's exposure to potential threats. Based on these findings, tailored remediation measures were proposed according to EMAPA’s technical and operational capabilities. These recommendations aim to strengthen system security, prevent incidents, and improve the management of technological risks.

Finally, the study highlights the importance of implementing regular cybersecurity controls on the organization's servers. The insights provided support informed technical and strategic decision-making in the protection of EMAPA's digital assets.

Keywords: Cybersecurity, vulnerabilities, servers, EMAPA, remediation.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

ANÁLISIS DE SEGURIDAD INFORMÁTICA SOBRE EL IMPACTO DE LAS VULNERABILIDADES EN LOS SERVIDORES INTERNOS DE EMAPA

1.1.1 Planteamiento del problema

A nivel mundial, las auditorías de seguridad de la información han pedido una relevancia netamente estratégica debido al crecimiento exponencial de las amenazas cibernéticas. En este punto las organizaciones están alineados sus políticas de seguridad con ciertas normas internacionales como son la ISO/EC 27001 y NIST (Instituto Nacional de Estándares y Tecnologías) como medio para salvar la respectiva información. Las empresas de todos los sectores están teniendo atacadas de manos cada vez más sofisticadas, lo que indica la necesidad de evaluaciones regulares d vulnerabilidades para enfrentar y establecer la mitigación de los riesgos significativos que podrían comprometerse potencialmente la infraestructura tecnológica y la información sensible [1].

Particularmente en América Latina, las empresas de los servicios públicos han sido particularmente un objeto de mayor ataque dirigido, lo cual buscan explotar debilidades en los respectivos servidores y redes que en ciertas ocasiones cuidan de la monitorización adecuada [2].

En contextos empresariales, el término se logra aplicar comparativamente a configuraciones se los servidores deficientes que relativamente lo hacen vulnerables a ataques. Los servidores actuales a menudo se cumplan por una amplia variedad de brechas que aprovechan maliciosamente las vulnerabilidades de seguridad de los servicios prestados. Esto no solo pone en riesgo la información, sino que también aumenta el tiempo de inactividad, lo que afecta la continuidad operativa y expone a la empresa a riesgos graves [3].

La empresa EMAPA, que se encuentra en la ciudad de Ambato, se destaca por una reconocida labor social y su importante contribución en el ámbito a la comunidad. Prácticamente su trabajo incorpora un registro eficiente de usuarios y la instalación de nuevas instalaciones en áreas previas estudiadas por el personal técnico de la institución, lo que netamente garantiza un servicio de calidad que atiende las necesidades de la población.

1.2 Antecedentes investigativos

A través del examen de diversas fuentes de investigación científica y académica. Las respectivas cadenas de búsqueda se configuraron para capturar búsquedas claras y precisas, teniendo en cuenta palabras clave como: Vulnerabilidades, impacto, Tecnología de la Información, auditoría y empresas, en tres tipos de bases de datos académicas referidas como Scielo, IEE EXPLORE y Google Scholar. Estas investigaciones de búsqueda presentadas están reflejadas en los periodos de tiempo desde 2019 hasta 2024. En la que se presenta una tabla con los resultados correspondientes a continuación.

Tabla 1. Cadenas de Búsqueda aplicadas en base de datos científicas

Base de datos	**Cadenas de Búsqueda**	**Núm. De Artículos**
Scielo	(TITLE-ABS-KEY(VULNERABILITY) ANDTITLE-ABS-KEY (IN THE ORGANIZATION)) ANDPUBYEAR > 2018-2023	72
IEEE Xplore	(TITLE-ABS-KEY(AUDIT) AND TITLE-ABS-KEY (COMPUTER SECURITY)) AND PUBYEAR > 2020	11
Google Scholar	Seguridad Informática Vulnerabilidades "Impacto" 2019-2023	17
	Total	100

Además, la búsqueda se amplió navegando en repositorios académicos de instituciones en Ecuador como la Universidad Técnica de Ambato, Universidad Politécnica Salesiana, Universidad Central del Ecuador, Universidad Militar de las Fuerzas Armadas (ESPE) y finalmente en la Universidad de Cuenca dentro del marco temporal filtrado de 2019 a 2024. Estos son los resultados mostrados en la tabla 2.

Tabla 2. Filtro de búsqueda aplicado en repositorio de universidades de Ecuador

	Filtro de Búsqueda	**Núm. De Artículos**
Universidad Técnica de Ambato	Seguridad informática y auditoría de sistemas	120
Universidad Politécnica Salesiana	Evaluación de vulnerabilidades en infraestructura TI	90
Universidad Central del Ecuador	Gestión de vulnerabilidades y ciberseguridad	75
Universidad de las Fuerzas Armadas ESPE	Auditorías de seguridad informática en servidores	60
Universidad de Cuenca	Impacto de vulnerabilidades en sistemas informáticos	85
	Total	430

Al final de esta revisión de la literatura, el autor tiene el beneficio de ofrecer un análisis que esté relacionado con temas de seguridad y debilidades para realizar un análisis de seguridad informática en los servidores internos de EMAPA. En este proceso, se emplearon algunos criterios de inclusión y exclusión y de manera concluyente, se especifica que hay 15 artículos que cumplen con la información necesaria en la que se consideran más importantes para desarrollar una investigación teórica fundamentado dentro del proyecto de investigación.

Tabla 3. Criterios de Inclusión y Exclusión

Inclusión	• Los respectivos articulos tratan específicamente sobre la seguridad y como controlar las vulnerabilidades • Las investigaciones enfatizan sobre como implementan análisis y desarrollan nuevas formas para evitar los riesgos de vulnerabilidades. • Artículos que realmente aborden ciertos desafíos y nuevas opciones de solución para el tema evaluar el impacto de vulnerabilidades en diferentes empresas a nivel global.

Exclusión	• Se enfoca en estudios que no logren centrarse en la seguridad informática para ciertas empresas. • Investigación de artículos que aborda temas sobre la inversión económica al implementar nuevas tecnologías. • Artículos que no se encuentren relacionados con la seguridad informática dentro de una organización específica.

En estudios recientes realizados sobre la ciberseguridad de pequeñas y medianas empresas (PYMES) en Colombia, se destacó un nivel notable de atención hacia la evaluación y control del nivel de debilidad en relación con ciberataques. Uno de los estudios discutidos en la base de datos Scielo Chile [4] abordó estos temas y mostró cómo las PYMES suelen estar en considerable peligro porque no hay recursos asignados para la seguridad cibernética. Este estudio aplicó un enfoque de encuesta y auditoría para establecer el grado de preparación de estas empresas, con el resultado de que la mayoría de ellas tenía políticas de seguridad débiles y eran, por lo tanto, como consecuencia de esas políticas, la mayoría de las personas eran víctimas o fácilmente podían ser victimizadas. Además, se hizo hincapié en abordar el cierre de cajas especialmente diseñadas teniendo en cuenta la falta de fondos presupuestarios y personal competente para lidiar con la seguridad en el campo de tecnologías de la información y comunicación.

Por medio de este estudio correspondió al departamento de Boyacá en Colombia, quien se encargó de una empresa privada, utilizando una de sus metodologías que comprendía la gestión de vulnerabilidades a través de la identificación, clasificación y priorización de las amenazas utilizando herramientas de análisis de seguridad [5]. Como resultado, este estudio resaltó la necesidad de la auditoría periódica de los sistemas informáticos y la adopción proactiva, como la modernización continua del software y los Sistemas de Detección de Intrusos. El uso de estas prácticas por las empresas mostró cambios recientes y favorables en la resistencia de la infraestructura tecnológica.

El gemelo digital es uno de los métodos más integrados y modernos de software. Esta tecnología proporciona, como se ha documentado en un artículo de IEEE Xplore [7], una representación virtual precisa que puede ser consultada a través del monitoreo y análisis en tiempo real, permitiendo a los sistemas informáticos brindar seguridad a los

usuarios que los utilicen. Su implementación, en el caso de los entornos empresariales, tiene el potencial de cambiar el paradigma en cuanto a las alertas y la respuesta a las amenazas cibernéticas empleando tecnologías de defensa más eficaces.

Se investigaron las vulnerabilidades de seguridad informática existentes en los servidores de una empresa privada en Bogotá, Colombia, utilizando herramientas de análisis específicas para prevenir y mitigar riesgos [6]. Esta actividad destacó la necesidad de un enfoque integral a la seguridad que incluya, como mínimo, auditorías de seguridad, evaluaciones de vulnerabilidad y formación para el personal en higiene básica de ciberseguridad. Los datos obtenidos fueron inequívocos: la aplicación de estos mecanismos ayudó a lograr una mejora en la seguridad de datos y una consolidación de la infraestructura tecnológica.

El propósito de estos trabajos de investigación es mostrar la situación más reciente y los problemas que enfrentan las pequeñas y medianas empresas y las empresas privadas en Colombia en cuanto a la seguridad informática. Es evidente que la integración de nuevas tecnologías y la gestión efectiva de vulnerabilidades son esenciales para proteger los sistemas de información y mitigar las posibilidades de ciberataques.

1.3 Fundamentación teórica

1.3.1 Tecnologías de las Información

Dentro de esta área profesional se refiere a un conjunto de herramientas y una arquitectura diseñados para gestionar, procesar una determinada cantidad de datos. En un entorno empresarial, el uso de TI hace posible gestionar la información empresarial y realizar automáticamente procesos críticos, lo que aumenta la eficiencia de la organización y mejora la toma de decisiones en tiempo real. La implementación de TI en las organizaciones tiene como objetivo aumentar la productividad, mejorar la comunicación interna e interorganizacional y proporcionar una gestión de información adecuada y eficiente. Las TI son importantes para el establecimiento y mantenimiento de una infraestructura sólida que soporte el funcionamiento sincronizado de todas las

unidades operativas hacia los objetivos estratégicos de la organización, ya que cubren todo el espectro que va desde hardware, software y redes de comunicación.

1.3.2 Seguridades

La ciberseguridad es un componente crucial dedicado a la protección de los activos digitales contra riesgos internos y externos. Se concentra en tomar acciones y controles que protejan la confidencialidad, integridad y disponibilidad de la información. Esto abarca la identificación de debilidades, la gestión de riesgos y la adopción de un curso de acción preventivo y correctivo para mitigar la posibilidad de que ocurra un incidente. Un sistema de seguridad efectivo no solo toma medidas contra ataques potenciales, sino que también anticipa futuras amenazas mediante la vigilancia activa y toma medidas proactivas constantes, asegurando la continuidad operativa del negocio y la confianza en los entornos tecnológicos [14].

1.3.3 Análisis de Servidores

Considerando la administración como un dominio tan amplio y complejo, el análisis de servidores es considerado una práctica clave no solo en la operación y seguridad, sino también en la resolución de problemas que afectan la calidad de la información, ya que busca la definición, valoración y mitigación de posibles riesgos en la vulnerabilidad de los sistemas en torno a la infraestructura tecnológica. Esto involucra la revisión de la actividad de configuración, el control de los parches y el monitoreo de la actividad para detectar anomalías. En esta supervisión existe la intención de proteger la integridad y disponibilidad de los datos, así como tratar la educación de posibles fallas del sistema que pueden ser utilizados por amenazas dentro o fuera de la organización. La seguridad informática se sostiene sobre el análisis de logs y la realización de escaneos periódicos que permiten decidir un refuerzo de protección del entorno ante un entorno digital en continuo cambio [11].

1.3.4 Auditoría de Seguridad Informática

Dentro del ámbito de la protección informática es un proceso meticuloso que intenta evaluar el nivel de riesgo para los sistemas de información de una organización,

buscando amenazas y vulnerabilidades. Esta auditoría requiere un examen extenso de las políticas de seguridad, control de acceso y gestión, configuración de red y aplicación, así como cumplimiento de leyes, regulaciones y estándares de seguridad. El objetivo principal de tal auditoría es detectar riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de los datos. Además, la auditoría ayuda a formular una estrategia de control para mejorar la protección de la tecnología de información del sistema, aumentando las posibilidades de frustrar intentos de ataques exitosos mientras limita el daño de cualquier brecha de seguridad que pueda ocurrir [13].

1.3.5 Seguridad de la Información

La seguridad de la información se refiere a una categorización de políticas, procesos y herramientas que tienen como objetivo defender la confidencialidad, integridad y disponibilidad de los datos en una organización. Menciona todo, desde la gestión de riesgos de acceso no autorizado hasta los controles técnicos y organizativos que pueden prevenir la pérdida o modificación de información crucial. Cuanto más dinámico se vuelve el mundo digital, más proactiva tiene que volverse la seguridad de la información, fusionando tecnologías avanzadas, auditorías regulares y capacitación constante del personal para lidiar con nuevas amenazas. Tal enfoque va más allá de la limitación de riesgos; mejora la resiliencia operativa y la confianza de los interesados [15].

1.3.6 Automatización y Control de Servidores

La automatización y el control de servidores es un gran paso adelante en el control y la gestión de una infraestructura tecnológica. Con la implementación de sistemas de monitoreo y mantenimiento automatizados, las empresas, en general, logran una mejora en la disponibilidad y la fiabilidad de sus servidores, al tiempo que reducen la probabilidad de interrupciones en el servicio. Un sistema de control automatizado facilita una gestión más eficiente de los recursos del sistema al optimizar el consumo de CPU, memoria y almacenamiento. Además, la automatización ayuda a identificar y corregir fallas, así como a instalar actualizaciones de software y parches de

seguridad. Esto ayuda a asegurar que los servidores funcionen dentro de los parámetros definidos, con el objetivo de ayudar a la organización a cumplir su meta de proporcionar servicios ininterrumpidos y seguros [12].

1.3.7 Mitigación de Vulnerabilidades

La mitigación de vulnerabilidades es necesaria para prevenir que los sistemas de información y los datos críticos de una empresa sean amenazados desde dentro y fuera. Esto implica identificar, medir y rectificar las brechas y debilidades en la infraestructura de servidores y redes, lo que minimiza las posibilidades de incidentes de ciberseguridad, como el acceso no autorizado. La aplicación de medidas de mitigación, incluidas la implementación de actualizaciones de parches de seguridad, el endurecimiento de la configuración de red y la autenticación fuerte ayuda a mantener la confidencialidad y la integridad de la información de la respectiva empresa. La mitigación de vulnerabilidades es una tarea proactiva y continua que otorga a una organización la capacidad de adoptar una postura de seguridad fuerte, al tiempo que reduce la probabilidad de violaciones de seguridad y asegura la disponibilidad continua de los servicios [14].

1.3.8 Eficiencia Operativa

La eficiencia operativa resulta esencial para cumplir metas de forma efectiva y rentable, logrando un mejor uso de los recursos disponibles. Alcanzar la eficiencia operativa requiere de la optimización en la utilización de equipos, energía y recursos humanos para que cada proceso y recurso se lleve a cabo de la forma más efectiva posible. La mejora en la eficiencia, por un lado, no solo le permite a la empresa optimizar costos, sino también aumentar la efectividad de su respuesta a las necesidades de la comunidad. En EMAPA, la eficiencia operativa es crucial porque favorece la competitividad de la organización al permitirle brindar servicios de calidad a bajo costo, lo cual redunda en beneficios al ecosistema y a la comunidad.

1.4 Objetivos

1.4.1 Objetivo general

Realizar un análisis de seguridad informática sobre el impacto de las vulnerabilidades en los servidores internos de EMAPA.

1.4.2 Objetivos específicos

- Realizar un levantamiento de activos tecnológicos de los servidores internos de EMAPA.
- Determinar la herramienta más adecuada para el análisis de seguridad informática, considerando su capacidad para identificar y clasificar vulnerabilidades.
- Detectar las vulnerabilidades presentes en los servidores internos de EMAPA y proponer medidas de remediación.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para recolectar información para el presente proyecto se utilizó herramientas como una encuesta para todo el personal del área de Tecnologías de la Información de la empresa EMPA, una entrevista para la persona encargada de la misma y además de una ficha de observación. Estas herramientas permitieron obtener datos relevantes sobre los procesos actuales, necesidades y desafíos del negocio. La combinación de métodos cualitativos y cuantitativos facilitó una visión integral para el diseño del sistema propuesto.

a) Encuesta al departamento de Tecnologías de la Información de la empresa "EMAPA"

Objetivo: Evaluar el nivel de conocimiento, prácticas actuales y percepción del personal del departamento de TI de EMAPA sobre la seguridad informática, con énfasis en la gestión de vulnerabilidades en los servidores internos.

SECCIÓN 1: Datos Generales

1. **Cargo que ocupa en el Departamento de TI:**

- Jefe de TI
- Administrador de Sistemas
- Especialista en Seguridad Informática
- Desarrollador de Software
- Otro: _____.

2. **Años de experiencia en el área de TI:**

- Menos de 1 año
- 1 - 3 años
- 4 - 6 años
- Más de 6 años

SECCIÓN 2: Conocimiento sobre Seguridad Informática

3. **¿Con qué frecuencia se realizan análisis de seguridad en los servidores internos?**

- Mensualmente
- Trimestralmente
- Semestralmente
- Anualmente
- No se realizan análisis de seguridad

4. **¿Qué herramientas conoce o utiliza para la detección de vulnerabilidades? (Puede seleccionar más de una opción)**

- OpenScap
- Nessus
- Nmap
- OpenVAS
- Otras: _____

5. **¿Ha recibido capacitación formal en temas de seguridad informática y gestión de vulnerabilidades?**

- Sí
- No

SECCIÓN 3: Gestión de Vulnerabilidades y Procedimientos Actuales

6. **¿Existe un procedimiento establecido en EMAPA para la corrección de vulnerabilidades?**

- Sí, está documentado y se aplica de forma estricta
- Sí, pero no se aplica con regularidad
- No, no hay un procedimiento definido

7. **¿Qué tipo de acciones o prácticas se aplican actualmente para proteger los servidores internos de la empresa? (Puede seleccionar más de una opción)**

- Se limita el acceso solo al personal autorizado
- Se revisa periódicamente la configuración de seguridad
- Se utilizan programas para monitorear la red
- Se controla el uso de los sistemas por parte del personal
- Otras: _____

8. **¿Cómo se priorizan actualmente las vulnerabilidades detectadas?**

- Por nivel de criticidad (alta, media, baja)
- Por tipo de servicio o proceso afectado
- No existe un criterio de priorización

SECCIÓN 4: Impacto de Vulnerabilidades en los Procesos Críticos

9. **¿Qué procesos considera que serían más afectados en caso de un ataque o vulnerabilidad crítica? (Puede seleccionar más de una opción)**

- Sistema de Facturación
- Sistema de Gestión de Clientes
- Sistema de Control de Inventarios
- Sistema de Gestión Financiera
- Otro: _____

10. **¿Ha ocurrido anteriormente alguna interrupción en los servicios debido a fallos de seguridad informática?**

- Sí
- No

11. **En caso afirmativo, ¿cuál fue el impacto principal?**

- Pérdida de información
- Interrupción del servicio
- Acceso no autorizado a datos
- Otro: _____

SECCIÓN 5: Opinión y Sugerencias

12. **¿Considera que el Departamento de TI cuenta con los recursos suficientes para proteger los servidores internos de EMAPA?**

- Sí
- No
- Parcialmente

A continuación, se logra demostrar el formato de una entrevista dirigido hacia el Jefe de Tecnologías de la Información de la empresa EMAPA.

b) Guía de entrevista dirigido al Jefe de departamento de Tecnologías de la información en la empresa EMAPA

Objetivo de la entrevista: Recopilar información técnica y experiencial del personal del departamento de TI de EMAPA sobre las prácticas actuales de protección en servidores físicos y virtuales, con el propósito de detectar posibles debilidades en la infraestructura informática y comprender los riesgos que perciben como más relevantes en su entorno de trabajo.

1. ¿Qué tipo de servidores administran actualmente y qué funciones cumple cada uno (físicos y virtuales)?
2. ¿Cuáles son los mecanismos que utilizan para controlar el acceso a los servidores, tanto a nivel físico como lógico?
3. ¿Existen procedimientos establecidos en caso de incidentes de seguridad? Si no, ¿cómo suelen actuar en esos casos?
4. ¿Se han identificado o enfrentado vulnerabilidades en los últimos meses? ¿Cómo se manejaron?
5. ¿Utilizan herramientas para monitorear la seguridad de los servidores y detectar amenazas? ¿Cuáles?
6. ¿Existe documentación formal sobre políticas de seguridad informática en la empresa? ¿Está al alcance del equipo?

7. Desde su experiencia, ¿cuál considera que es el mayor riesgo actual para la seguridad de los servidores de EMAPA?

A continuación, específicamente se logra identificar una ficha de observación, en el cual permite llevar a cabo un registro de los diferentes aspectos que consolida una observación de manera directa mediante los respectivos análisis de seguridad informática. Esta herramienta tiene el respectivo beneficio en recolectar una información netamente detallada sobre los fundamentos diarios que atraviesa en el tema de la seguridad de la información.

c) Ficha de observación – Evaluación de seguridad informática

Objetivo: Verificar la implementación de buenas prácticas de la seguridad informática mediante el respectivo manejo de los servidores físicos y virtuales del departamento de Tecnologías de la Información.

Tabla 4. Ficha de Observación

Ítem Observado	**Sí**	**No**	**Observación**
Acceso físico a los servidores controlados			Descripción
Documentación visible sobre las políticas de seguridad			Descripción
Señalización de las áreas restringidas			Descripción
Cámaras de seguridad en el área de los servidores internos			Descripción
Sistemas de respaldo visibles o identificables			Descripción
Servidores etiquetados y organizados			Descripción
Conexiones de red ordenadas y protegidas			Descripción
Uso de software para monitoreo en tiempo real			Descripción
Prácticas de autenticación robustas observadas			Descripción
Estaciones de trabajo bloqueadas cuando están inactivas			Descripción

2.2 Métodos

Este estudio empleó un enfoque cuantitativo porque se realizó un análisis estadístico de los datos recopilados a través de una encuesta administrada a la muestra seleccionada.

2.2.1 Modalidad de la investigación

La presente investigación se contextualizó en la modalidad de investigación de campo y bibliográfica-documental.

Investigaciones de campo

Dentro del alcance de esta investigación, se prestará especial atención a la parte de investigación de campo, que a diferencia de las otras partes permitirá una interacción relativamente directa con el entorno de sistemas de los servidores internos de EMAPA. Esto permitirá la recopilación de datos sobre las vulnerabilidades existentes, junto con la posibilidad de realizar análisis detallados de las configuraciones de seguridad y las medidas que se encuentran en los servidores para incidentes de seguridad.

Investigación bibliográfica – documental

En este caso particular, se llevará a cabo una investigación bibliográfica-documental con el objetivo de recopilar información relevante sobre la seguridad informática y los dominios de auditoría de sistemas. Con este enfoque, será posible revisar estudios anteriores y los marcos teóricos relevantes, así como estándares aplicables y regulaciones de seguridad para la gestión de vulnerabilidades en infraestructuras críticas. Se utilizarán documentos como artículos académicos, informes técnicos, legislación en seguridad de la información y guías de prácticas recomendadas para proporcionar contexto y justificación para los procedimientos de auditoría realizados, mejorando así el análisis y hallazgos hechos para disminuir los riesgos en los servidores internos de EMAPA.

2.2.2 Población y muestra

La población objetivo de este estudio considera al personal del Departamento de TI de EMAPA, así como a otros usuarios clave de TI que tienen contacto directo con el servidor interno de la empresa. Esto incluye una selección más amplia de personas, como profesionales y técnicos responsables de la administración, seguridad y soporte de los sistemas internos, lo que permite captar los procesos y la gestión de vulnerabilidades en el ecosistema tecnológico de EMAPA. La población total se

presenta en la Tabla 4, junto con los roles específicos y las contribuciones porcentuales que cada categoría realiza para el total de la población.

Tabla 5. Población de estudio

Población	Número	Porcentaje
Jefe de TI	1	20 %
Personal Operativo	4	80 %
Total	5	100 %

En este estudio se abordará directamente a todos los integrantes de la población, ya que su número total es inferior a cien personas. Debido a la cantidad limitada, no se aplicará un proceso de muestreo, sino que se considerará a la totalidad de los casos para el análisis, garantizando así una cobertura completa del grupo observado.

2.2.3 Recolección de información

Mediante del instrumento del método de Alfa de Cronbach netamente dirigido al departamento de TI de la empresa EMAPA.

En este proceso de cálculo se menciona el respectivo cálculo del coeficiente de Alfa de Cronbach en el cual es una medida estadística en la que es empleada para realizar una evaluación de confiabilidad o consistencia interna de un con determinado conjunto de ítems en una prueba o encuesta. Junto con su valor que relativamente oscila entre 0 y 1, donde un valor más alto que indica la mayor tendencia en la consistencia interna. Esto generalmente se logra utilizar por medio de la Escala Likert para realizar el enfoque respectivo en las estructuras de las preguntas, gracias a esto es una ayuda con alta fiabilidad para medir el mismo constructor o variable. Por otra parte, este coeficiente es relativamente crucial donde garantiza ciertos datos obtenidos mediante una determinada encuesta en la que sean representadas y estables, lo que generalmente aumenta una cierta validez de los respectivos análisis con los datos recolectados.

$$\boldsymbol{a = \frac{k}{k-1}\left[1 - \frac{\sum v_i}{vt}\right]}$$

Tabla 6. Cálculos de las Varianzas y Sumatorias

	Pregunta 1	**Pregunta 2**	**Pregunta 3**	**Pregunta 6**	**Pregunta 8**	**Pregunta 11**	**Pregunta 12**	**Suma**
Sujeto 1	1	4	4	3	2	1	2	17
Sujeto 2	4	2	4	3	2	1	2	18
Sujeto 3	6	4	3	3	2	1	2	21
Sujeto 4	5	4	2	3	1	4	3	22
Sujeto 5	5	4	5	2	3	5	3	27
Varianza	3.7	0.8	1.0	1.5	0.2	0.7	3.2	
Sumatoria varianza de ítems	11.1							
Varianza total del instrumento	32.3							

Tabla 7. Resutados estadisticos del coeficiente Alfa de Cronbach

a	coeficiente de confiabilidad	0.766
K	Número de ítems de instrumento	5
$\sum v_i$	Sumatoria de varianza de los ítems	11.1
vt	Varianza total del instrumento	32.3

Tabla 8. Interpretación de confiabilidad

Alfa de Cronbach	**Interpretación**
0,9 – 1	Excelente
0,8 – 0,9	Buena
0,7 – 0,8	Aceptable
0,6 – 0,7	Débil
0,5 – 0,6	Pobre
< 0,5	Inaceptable

Al obtener el resultado mediante el uso de la herramienta del Alfa Cronbach con un respectivo valor de 0.766 en la que generalmente se concluye con un nivel bueno de confiabilidad en la encuesta realizada.

Encuesta realizada

Mediante la realización de la presente encuesta al departamento de TI, donde forma parte de la empresa EMAPA, cuyo objetivo tuvo en lograr recopilar una determinada información sobre el conocimiento y planteamiento sobre la seguridad de la información dentro de los servidores internos de la organización empresarial. Las preguntas de la encuesta netamente son diseñadas para establecer un enfoque en la que abarca ciertos aspectos como el tipo de conocimientos que tiene el departamento de TI, las respectivas actividades en las que se puede aplicar en caso de que exista una desactualización dentro de los servidores, los años de experiencia que tiene cada personal en el área de trabajo y finalmente el tipo de control del personal en la que lleva a cabo el acceso a los servidores internos. Además, por media esta encuesta se buscó identificar el nivel de cocimiento junto a la parte experimental del personal de TI para llevar a cabo una remedición adecuada dentro de cada unos de los servidores internos que contribuye la infraestructura de la organización empresarial. Finalmente, los resultados obtenidos fueron muy fundamentales para llevar a cabo una mayor integridad hacia el análisis, identificación y una remedición teórica para el personal que administra cada uno de los servidores, garantizando que se lleva a cabo una optimización de vulnerabilidades y remediciones en cada una de ellas.

Pregunta 1: Cargo que ocupa en el Departamento de TI:

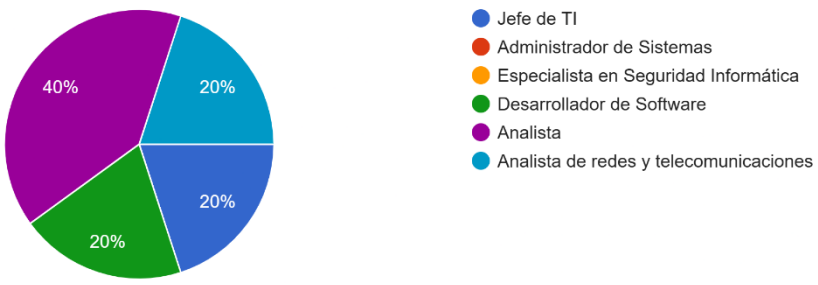


Figura 1. Cargo que tiene el personal de TI

Análisis e interpretación de los resultados

Mediante el análisis de la **Figura 1** muestra que un determinado porcentaje en cada uno de los cargos que ocupa el personal dentro del departamento TI, lo que indica que el porcentaje más elevado es de (40%) sobre el personal que tiene el cargo de analista. Sin embargo, el (20%) del personal encuestado forma parte del jefe de TI, el siguiente porcentaje es de (20%) en la que se lleva a cabo los cargos de analista de redes y telecomunicaciones, junto al cargo de un desarrollador de software, esto llega a la conclusión que dentro del departamento de TI existe un jefe del área en la que conlleva las respectivas organizaciones, actividades, planteamiento, actualizaciones de las horas de trabajo del personal. Esto generalmente podría influir en una mayor precisión en otorgar el acceso hacia los servidores internos a personal con el enfoque claro tomando en cuenta su cargo respectivo.

Pregunta 2: Años de experiencia en el área de TI:

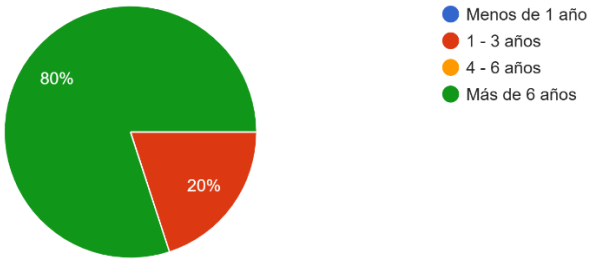


Figura 2. Identificación de los años de experiencia del personal de TI

Análisis e interpretación de los resultados

El análisis de la **Figura 2** se lleva a cabo un porcentaje alto del (80%), lo cual significa que el personal del área de Tecnologías de la Información tiene “Más de 8 años” de experiencia con un conocimiento estable y organizacional. Por otra parte, no se llevaron a cabo los resultados de una experiencia intermedia o básica con un porcentaje del (20%), lo cual significa que el personal que forma parte dentro los horarios laborales del departamento de TI obtienen un aporte claro y eficaz junto a su alta experiencia.

Pregunta 3: ¿Con que frecuencia se realizan análisis de seguridad en los servidores internos?

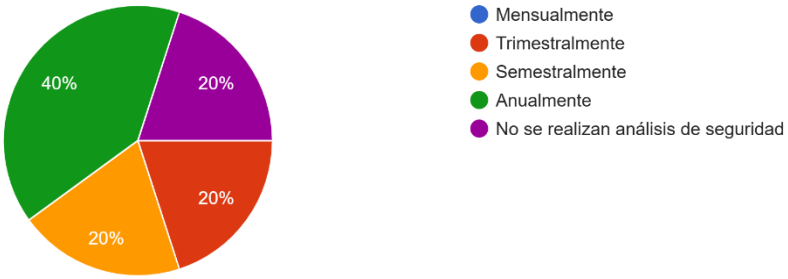


Figura 3. Frecuencia de los análisis de seguridad en los servidores internos

Análisis e interpretación de los resultados

Por medio del análisis de la **Figura 3** logra mostrar un 40% de las respuestas significa que los análisis de seguridad de la información los realizan anualmente, mientras que el 20% ejecutan semestralmente, trimestralmente y otros no se realizan análisis de seguridad. Estos resultados precisamente destacan que existe un porcentaje de escaneo entre cuatro factores específicos que generalmente se considera no muy estable ya que por dejar de realizar un cierto tiempo los escaneos. Estos resultados relativamente se destacan como algo en condiciones críticas ya que en parte el personal del departamento de TI aporta con mayor eficacia sus conocimientos de análisis de seguridad después de un cierto tiempo específico durante el año laborable.

Pregunta 4: ¿Qué herramientas conoce o utiliza para la detección de vulnerabilidades?

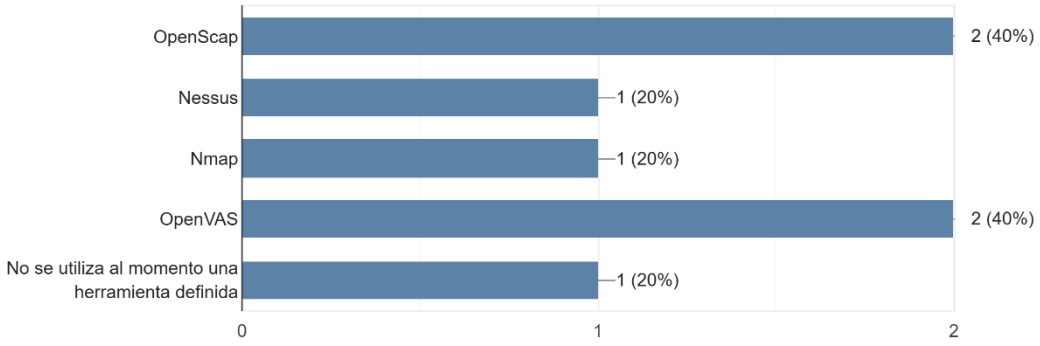


Figura 4. Herramientas de la detección de vuleabilidades

Análisis e interpretación de los resultados

Generalmente esto indica que las herramientas que más son utilizadas por parte del personal de Tecnologías de la información para los análisis de seguridad en los servidores internos precisamente se evalúan en dos porcentajes, un 40% en la que utilizan las herramientas como OpenScap y OpenVas, la otra parte de porcentaje es de un 20% que se derivan en la utilidad de Nessus, Nmap y ninguna otra herramienta. Lo que significa que cada uno de los integrantes que forma parte del departamento de TI, tiene su adecuado conocimiento para aplicar las herramientas específicas en los análisis de seguridad informática.

Pregunta 5: ¿Ha recibido capacitación formal en temas de seguridad informática y gestión de vulnerabilidades?

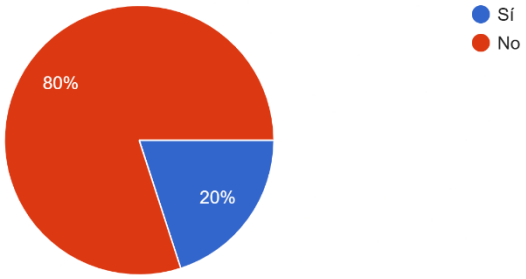


Figura 5. Capacitación informática y gestión de vulnerabilidades

Análisis e interpretación de los resultados

Mediante este análisis se logra identificar que el personal del área de TI no ha recibido una capacitación adecuada sobre la seguridad informática y la respectiva gestión de vulnerabilidades con un porcentaje desfavorable del 80%. Esto significa que el departamento de Tecnologías de la información debe consolidarse en estudiar y asistir aun pequeña capacitación lo cual es de suma importancia para tenga en cuenta la seguridad ya que dentro la infraestructura de EMAPA manejan ciertos servicios de mayor importancia para el funcionamiento de aplicativos, sistemas y almacenamientos de datos del registro de usuarios.

Pregunta 6: ¿Existe un procedimiento establecido en EMAPA para la corrección de vulnerabilidades?

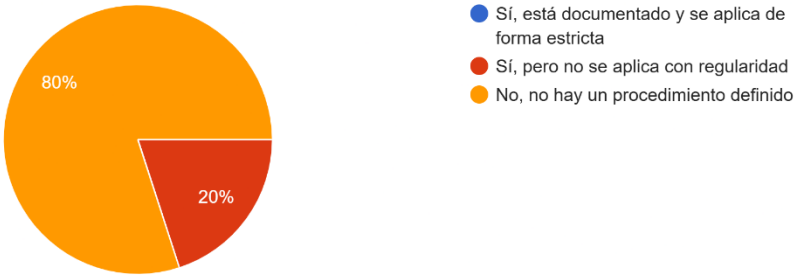


Figura 6. Corrección de las vulnerabiliades en EMAPA

Análisis e interpretación de los resultados

La pregunta 6 como específicamente indica la **Figura 6**, garantiza que no existe un procedimiento definido, de tal manera que esto se llega a un porcentaje del 80% de los encuestados y el 20% que generalmente no se aplica en los servidores de EMAPA una corrección específica. Pero en base a ciertas vulnerabilidades que surge en ciertos casos de los servidores de mayor importancia de la infraestructura debería sera aplicable las correcciones adecuadas con una mayor configuración eficiente y técnica.

Pregunta 7: ¿Qué tipo de acciones o prácticas se aplican actualmente para proteger los servidores internos de la empresa?

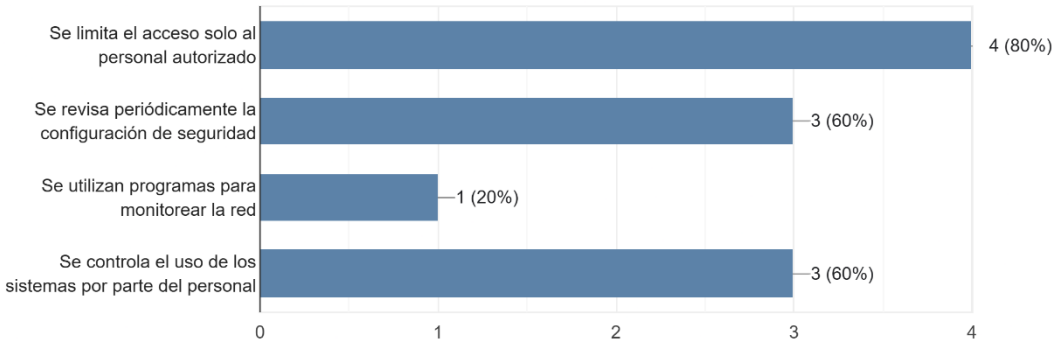


Figura 7. Acciones o prácticas que se aplican para proteger los servidores internos

Análisis e interpretación de los resultados

Generalmente, las acciones para el acceso a los servidores de EMAPA se tiene un personal autorizado, lo cual especifica y garantiza un mayor complemento para los análisis y controles de seguridad informática. Esto se lleva a cabo con un 80% que lleva a los casos satisfactorios con una integridad relevante hacia la protección de los servidores internos.

Pregunta 8: ¿Cómo se priorizan actualmente las vulnerabilidades detectadas?



Figura 8. Priorización de las vulnerabilidades detectadas

Análisis e interpretación de los resultados

En el caso de la identificación de las vulnerabilidades se destaca en esta pegunta con un porcentaje alto del 60%, donde principalmente priorizan el afecto de los tipos de servicios o procesos adecuados, lo cual son fundamentales para brindar un informe de remediación con pasos y enfoques técnicos.

Pregunta 9: ¿Qué procesos considera que serían más afectados en caso de un ataque o vulnerabilidad crítica?

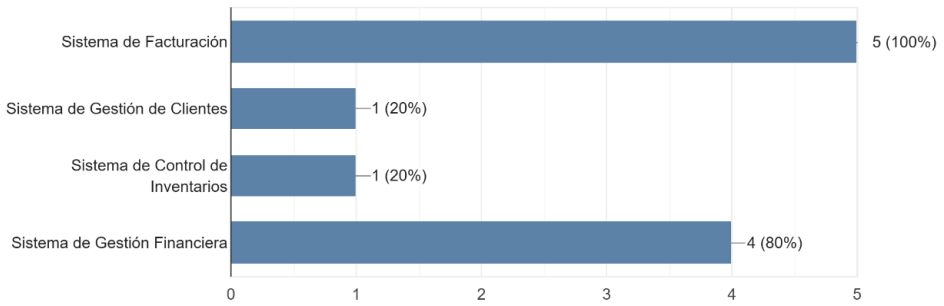


Figura 9. Procesos que sean los más afectados contra una vulnerabilidad crítica

Análisis e interpretación de los resultados

Durante identificación de las vulnerabilidades de mayor criticidad del 100% en los sistemas de facturación en la que manejan dentro de la institución, lo cual significa que considera de los servicios más afectados si llega el caso de surgir una vulnerabilidad de alto riesgo. Por otra parte, se tiene un 80% que corre el riesgo en los sistemas financieros, y finalmente los que se consideran un porcentaje menor del 20% son los sistemas de gestión de clientes y las gestiones de inventarios. Esto generalmente se logra visualizar de manera estadística los procesos en las cuales se pueden tomar medias para remediar problemas, que afecten a los servidores internos.

Pregunta 10: ¿Ha ocurrido anteriormente alguna interrupción en los servicios debido a fallos de seguridad informática?

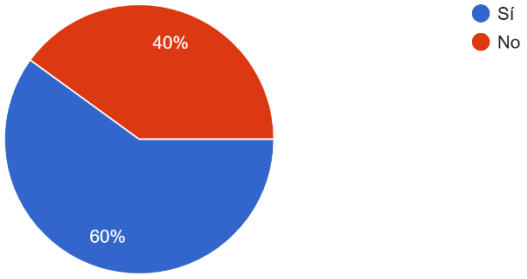


Figura 10. Servicios a fallos de seguridad informática

Análisis e interpretación de los resultados

Específicamente, lo que se demuestra en la Figura 10 da a conocer que ha existido un 60% de interrupciones de los servicios que ejecuta los servidores internos, donde analíticamente se define que existen una falta de actualización del sistema operativo, configuración técnica aplicando ciertas condiciones de los servicios que proporcionan los servidores para la utilidad de forma interna y externa en la empresa EMAPA.

Por otro lado, el 40% proporciona la información que o ha ocurrido una mayor complejidad de las interrupciones en los servicios de la seguridad informática que contiene los respectivos servidores internos dentro del departamento de Tecnologías de la Información.

Pregunta 11: En caso afirmativo, ¿Cuál fue el impacto principal?

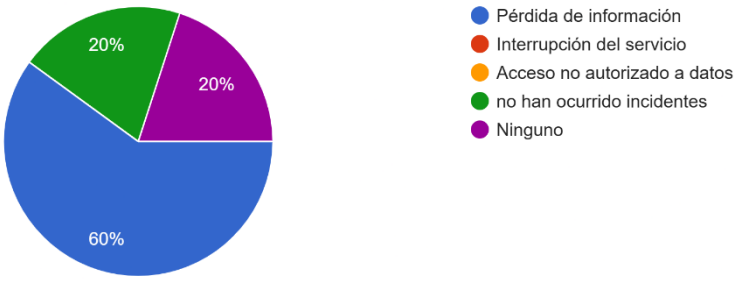


Figura 11. Impacto principal

Análisis e interpretación de los resultados

La presente que se visualiza en la Figura 11, da a conocer el impacto principal de un 60 %, en la que se da a conocer como "Pérdida de información", esto se interpreta que por medio de las desactualizaciones de cada uno de los servidores surgen ciertas configuraciones en las que son desfavorables para la infraestructura de TI, junto al persona que tiene un acceso limitado para controlar con una mayor integridad de seguridad informática.

Pregunta 12: ¿Considera que el Departamento de TI cuenta con los recursos suficientes para proteger los servidores internos de EMAPA?

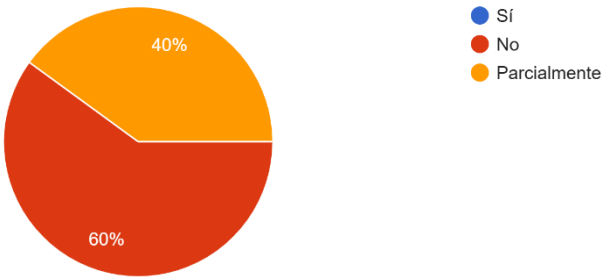


Figura 12. Recursos suficientes para proteger los servidores internos de EMAPA

Análisis e interpretación de los resultados

Generalmente existe el 60% en la que se considera que del departamento de Tecnologías de la información no obtiene los recursos necesarios para reforzar las medidas de seguridad contra vulnerabilidades de alta criticidad.

Entrevista

Mediante otro método para obtener información precisa se realizó una entrevista en la que generalmente se beneficia una obtención de ciertos datos de información, con la finalidad que sea netamente detallada sobre el impacto de las vulnerabilidades en los servidores internos de EMAPA.

1. **¿Qué tipo de servidores administran actualmente y que funciones cumple cada uno de los servidores internos?**

Actualmente se ejecuta una administración de los servidores internos de manera física y virtualizados. Generalmente entre ellos se logran destacar como son los servidores de archivos, base de datos, controladores de un dominio, servidor de correo electrónico institucional de la empresa y las aplicaciones internas que existen.

Los servidores de archivos generalmente se tratan sobre un ámbito central para gestionar ciertos documentos institucionales facilitando así al personal que trabaja en la empresa con un acceso seguro y de forma ordenada.

El servidor de almacenamiento de las bases de datos que contiene la organización empresarial donde logra gestionar una determinada información de los empleados que aborda específicamente en los sistemas de gestión, sistemas comerciales junto al financiero y finalmente para el área de los recursos humanos. Los servidores que conlleva el controlador de un dominio se ejecutan por medio de una administración frecuente con las cuentas de usuario, las políticas de seguridad y el respectivo acceso de los recursos compartidos por medio de la red específica.

En el caso del servidor de correo se ejecuta la comunicación de una información de manera interna y externa.

Finalmente, se tiene lo que es el servidor de los aplicativos en la que se realiza el enfoque del soporte de ciertas herramientas web y los sistemas administrativos relativamente personalizados.

2. **¿Cuáles son los mecanismos que utilizan para controlar el acceso a los servidores, tanto a nivel físico como lógico?**

En el caso del nivel físico, los respectivos servidores se encuentran ubicados en el departamento de Tecnologías de la Información, bajo un ambiente controlado de temperatura y con un acceso restringido únicamente para el personal autorizado. Este tipo de acceso conlleva a tener cerraduras de seguridad manuales y cámaras de vigilancia.

Mediante al otro punto del control lógico, se usa por medio de una autenticación de acceso al departamento de TI con accesos remotos y las políticas de las contraseñas relativamente robustas para una segmentación de la red. Además, se logra aplicar ciertos roles y privilegios, donde se enfoca en el registro de las sesiones y registros de auditoría determinada.

3. **¿Existen procedimientos establecidos en caso de incidentes de seguridad? Si no, ¿cómo suelen actuar en esos casos?**

Sí, contamos con un cierto protocolo básico para el gestionamiento de incidentes. Esto generalmente incluye a la detección de los respectivos análisis, erradicación, y las recuperaciones del incidente, lo que conlleva a brindar un reporte a gerencia de la organización empresarial EMAPA. Por otra parte, estamos en el proceso de mejorar y fortalecer los planes de respuesta, que relativamente han surgido por lineamientos en la que permite actuar con mayor integridad y rapidez para aplicar las medidas correctivas inmediatas.

4. **¿Se han identificado o enfrentado vulnerabilidades en los últimos meses? ¿Cómo se manejaron?**

Sí, durante los últimos meses se lograron registrar en una detección de vulnerabilidades específicamente relacionadas con las configuraciones relativamente inseguras junto a las versiones que se encuentran relativamente desactualizadas de un software o del sistema operativo que administra un servidor interno. Estas se identificaron por medio la herramienta Nmap en el cual es la que generalmente se utiliza para los escaneos de las IPs que conlleva a la conectividad y verificación del estado de los servidores, lo cual se realizaron ciertos ajustes en la configuración

juntamente con la documentación que adiciona el fortalecimiento a la supervisión para evitar ciertas recurrencias.

5. **¿Por medio de las herramientas que utilizan para monitorear la seguridad de los servidores sea han detectado amenazas? ¿Cuáles?**

Si, herramientas como Nmap, OpenVas y el sistema de los registros que contiene firewalld donde han permitido en identificar ciertos intentos en el acceso no autorizados juntamente con los escaneos, para identificar ciertas amenazas comunes. Afortunadamente, ninguna de las vulnerabilidades que se han logrado encontrar dentro de los servidore internos han proporcionado un problema grande ya que los sistemas que se conlleva dentro de la organización empresarial tienen medidas preventivas en proceso de mejorar con más efectividad.

6. **¿Existe documentación formal sobre políticas de seguridad informática en la empresa? ¿Está al alcance del equipo?**

Actualmente se tiene una determinada política general por el respectivo uso aceptable de ciertas tecnologías con las normas basadas en la seguridad informática. Pero esto logra realizar el enfoque de reconocimiento de una documentación en la que debe actualizarse y ampliarse. En ciertos casos se está trabajando en realizar un manual más detallado dando a conocer las políticas y ciertos procesos de seguridad de la información. Mientras que mediante el equipo tiene la probabilidad de acceder por medio de lineamientos de una conexión de forma directa para ejecutar una solución sin ninguna duda y reportar ciertos incidentes.

7. **Desde su experiencia, ¿cuál considera que es el mayor riesgo actual para la seguridad de los servidores de EMAPA?**

Desde mi trayectoria en el área de Tecnologías de la Información, el mayor riesgo en la que generalmente hace falta una capacitación continua en ciertos temas que trate de la ciberseguridad, de tal manera que, aunque se tenga una infraestructura relativamente segura, ejecuta una acción incorrecta en la que puede exponer a toda la red de la organización empresarial. Por eso el objetivo primordial se enfocaría en aplicar una seguridad digital dentro de la organización, con la finalidad de prevenir con mayor prioridad los servidores internos con mayor control de acceso y actualizaciones.

Conclusión de la entrevista

La entrevista realizada en el departamento de Tecnologías de la Información, exclusivamente al Jefe del área, donde se revela un enfoque con mayor consistencia sobre el tema de la seguridad informática en la empresa EMAPA. Esto generalmente existe ciertos mecanismos sólidos en la que se considera controlar un acceso de manera física como lógica hacia el departamento de TI ya que los servidores internos se encuentran con una cerradura manual, en cuestión de la empresa logra reconocer ciertos ataques ejecutados por los factores humanos lo que genera ciertos riesgos de la seguridad en los sistemas que utilizan dentro de la organización empresarial. Mediante el tema de la identificación las vulnerabilidades el personal que trabaja en el área de Tecnologías de la Información demuestran un enfoque muy activo y dinámico para el gestionamiento de la seguridad, apoyado con ciertas herramientas que son factibles para monitorear y detectar vulnerabilidades en los servidores internos.

Para finalizar esta sección la empresa EMAPA está tomando ciertas medias de prevención, dando a conocer una mayor postura de seguridad que generalmente, son especializados con el procedimiento y la concientización de los empleados tomando en cuenta el tema de la ciberseguridad.

Ficha de Observación

Mediante la presente ficha de observación se llevó a cabo el análisis de una manera directa hacia la observación de la utilidad, el control, verificación y planteamientos de los servidores internos de EMAPA. Este enfoque generalmente fue permitido para identificar puntos en los que se puede remediar y fortalecer al momento de ejecutar medidas de seguridad en los servidores, con la finalidad de que el Jefe de TI proporcione una mejor visión integral en la parte de la seguridad informática.

Tabla 9. Resultados de la ficha de observación

Ítem Observado	Sí	No	Observación
Acceso físico a los servidores controlado	✓		El acceso al área de servidores está restringido al personal autorizado, garantizando la seguridad física de los equipos.
Documentación visible sobre las políticas de seguridad		✓	No se encontró documentación formal visible en el área. Sin embargo, se mencionó que está disponible en formato digital.

Ítem Observado	Sí	No	Observación
Señalización de las áreas restringidas	✓		Las áreas restringidas están adecuadamente señalizadas, asegurando que solo el personal autorizado pueda acceder a ellas.
Cámaras de seguridad en el área de los servidores internos	✓		Existen cámaras de seguridad en el cuarto de servidores, las cuales están funcionando correctamente.
Sistemas de respaldo visibles o identificables		✓	Los sistemas de respaldo no son fácilmente visibles, pero se mencionó que existen procedimientos establecidos para la realización de backups periódicos.
Servidores etiquetados y organizados	✓		Los servidores están debidamente etiquetados, facilitando su identificación y organización dentro del centro de datos.
Conexiones de red ordenadas y protegidas	✓		Las conexiones de red están bien ordenadas, con cables correctamente etiquetados y protegidos para evitar manipulaciones accidentales.
Uso de software para monitoreo en tiempo real	✓		Se utiliza la herramienta Nmap para monitorear la seguridad de los servidores en tiempo real.
Prácticas de autenticación robustas observadas	✓		Se observó el uso de autenticación multifactor para accesos remotos, y contraseñas seguras en el acceso a sistemas críticos.
Estaciones de trabajo bloqueadas cuando están inactivas	✓		Las estaciones de trabajo están configuradas para bloquearse automáticamente después de un período de inactividad.

Conclusión de la ficha de Observación

Los aspectos claves que se generó sobre los análisis de seguridad informática en los servidores internos de la empresa EMAPA, generalmente tiene sus ventajas y desventajas. En el cual se determina controles físicos de una manera más adecuada, lo que refuerza la seguridad física en el entorno del departamento de TI. Con una mayor integridad y seguramiento al momento de brindar los servicios a los usuarios que forman parte de la empresa.

Mediante ciertas medidas y análisis son fundamentales para llevar a cabo un claro fundamento de seguridad para que por medio de eso se lleve a cabo una remediación exclusiva con mayor objetividad en el informe con cada vulnerabilidad identificada en un proceso a futuro que ejecute el departamento de Tecnologías de la Información, llegando así al objetivo de brindar el conocimiento y apertura por medio las indicaciones generales del Jefe de TI junto a esta observación establecida de mayor énfasis en los análisis de vulnerabilidades de los servidores internos de la organización empresarial del agua potable.

2.2.4 Procesamiento y análisis de datos

Una vez realizado el proceso de la recolección de los datos de información se genera un análisis de los resultados obtenidos, utilizando un cuestionario para ejecutar el formato de encuestas, preguntas formuladas por el autor de este proyecto para ejecutar una entrevista y finalmente una ficha de observación para dar a conocer los puntos importantes del presente proyecto de investigación para realizar el enfoque de solución con una propuesta clara y consistente en el siguiente capítulo. En el caso de los procesamientos de los datos se realizará los posteriores escaneos de los 20 servidores que existen en la empresa EMAPA con la herramienta Nessus junto a un script de Nmap y finalmente para comprobación de cada vulnerabilidad OpenScap. A su vez, esto será favorable ya que con la ayuda de la herramienta de Power BI se implementará unos gráficos estadísticos más visuales para identificar las vulnerabilidades con mayor cantidad estadística en la que afecta a los servidores internos de EMAPA.

Desarrollo del Proyecto

Para dar el cumplimiento de los objetivos planteados de la presente investigación se presenta las siguientes actividades aprobadas:

1. Aplicar la metodología WSP
2. Levantamiento de activos tecnológicos
3. Selección de la herramienta de análisis de seguridad informática
4. Detección de vulnerabilidades y evaluación de su impacto
5. Diseño de medidas de remediación mitigación de riesgos
6. Análisis de los resultados sobre el impacto de las vulnerabilidades en los procesos críticos
7. Redacción de informe técnico de los resultados y recomendaciones específicas
8. Presentación del informe final al Jefe de TI

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

En este capítulo del proyecto de investigación específicamente va a tratar sobre la ejecución de la metodología WSP para llegar a una conclusión de un enfoque integral para analizar los servidores internos de la empresa EMAPA, para mejorar los respectivos sistemas de trabajo que conectan y se utilizando de forma interna y externa. Mediante a este análisis se va a proyectar reportes de las vulnerabilidades con mayor criticidad dentro de los servidores internos más utilizados, herramientas de escaneo para la identificación de las gestiones sospechosas y al finalizar esa perspectiva de trabajo gestionar una diseño de remediación una vez visualizado los datos de cada uno de los servidores internos en la que implica obtener un detalle de mayor seguridad informática dentro del sistema de trabajo para el personal que forma parte de la organización empresarial.

3.1.1 Aplicación de la Metodología WSP

A través de los análisis y discusión de cada una de las herramientas utilizadas anteriormente sobre el personal del departamento de TI en la empresa EMAPA, netamente es necesaria aplicar la metodología WSP lo cual sus siglas en inglés son "Work System Methodology", esto generalmente llega a ser aplicada por medio de una evaluación de seguridad informática y el determinado impacto de las vulnerabilidades en cada uno de los servidores internos que contiene la organización.

En este enfoque la metodología WSP forma parte uno de los más integrales y con mayor magnitud, en la que permite analizar los sistemas de trabajo que contiene cada uno de los servidores internos dentro de la organización específica, tomando en cuenta la distribución y las funcionalidades que se lleva a cabo el personal, los procesos, la tecnología que es utilizada y las estructuras organizacionales. Durante este contexto del presente proyecto den investigación, el sistema es acogido por medio de los ciertos objetivos dentro del sistema de trabajo en la que tiene el objetivo de conformar una infraestructura netamente tecnológica y operativa de la organización empresarial

EMAPA, tomando en cuenta un enfoque claro y consistente por medio de los aspectos de seguridad informática.

Generalmente el propósito satisface por medio de la aplicación de la metodología WSP, donde tiene el objetivo con una visión estructurada conforme al entorno de la seguridad informática que corresponde a la organización, identificando no solo el tema de las vulnerabilidades presentes en los servidores internos, sino también los diversos factores para las respectivas configuraciones que logran influir para la protección de la información con más detalle y con mayor seguridad. Por medio de este enfoque, se busca no solo en detectar y remediar las vulnerabilidades que se encuentran en cada uno de los servidores, sino también en fortalecer y optimizar en los diferentes sistemas de trabajo que contribuye la gestión de seguridad informática.

Para llevar a cabo la aplicación de la metodología redactada y estudiada en este capítulo se subdivide en varias fases que forma parte de una guía analítica y las soluciones teóricas que se va a implementar a continuación:

1. **Definición de los servidores internos:** Como primer paso se define la identificación y un levantamiento de activos de cada uno de los servidores del Data Center que se encuentra dentro del departamento de Tecnologías de la Información de la empresa EMAPA.

2. **Análisis de las interacciones y la evaluación de la tecnología:** Precisamente las herramientas y una evaluación comparativa de los mismos, donde se ejecuta por medio de ciertos escaneos y procesos que afectan la seguridad de los servidores internos.

3. **Identificación de las vulnerabilidades y diseño de soluciones:** Mediante las evaluaciones e interacciones identificadas, prácticamente se enfoca en diseñar las recomendaciones que promueven a remediar el problema de cada uno de los servidores para llegar al objetivo de mitigar ciertos riesgos con mayor prolongación.

4. **Implementación de los monitoreos visuales de los servidores:** En este punto se ejecuta graficas comparativas con cada uno de los servidores para

complementar el análisis tomando en cuenta cada vulnerabilidad de alta, media y baja criticidad que aes un fundamento técnico para llevar a cabo el análisis de la remediación.

5. **Evaluación y el enfoque de los análisis de los resultados:** Finalmente, en este punto se ejecuta una determinada evaluación de las medidas correspondientes, donde precisamente se llevará a cabo la mejora de la seguridad informática en los servidores internos para que los servicios que tiene instalado dentro de cada uno de ellos establezca una funcionalidad adecuada juntamente con los resultados obtenidos.

3.2 Desarrollo de la propuesta

3.2.1 Levantamiento de activos tecnológicos

Tabla 10. Levantamiento de activos servidores internos de EMAPA

Nombre	Tipo	Dirección IP	Sistema Operativo	Funcionamiento
Correo	Servidor	192.168.24.16	Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8	Virtualizado
SGB Documental	Servidor	192.168.24.85	Nutanix	Virtualizado
Comercial	Servidor	192.168.24.101	Linux Kernel 2.6	Virtualizado

BD Comercial	Servidor	192.168.24.102	Linux Kernel 2.6	Virtualizado
Administrativo	Servidor	192.168.24.88	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Virtualizado
Dominio SSL	Servidor	192.168.24.83	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Virtualizado
BD Administrativos	Servidor	192.168.24.84	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Virtualizado
Servicios en Línea	Servidor	192.168.24.62	Microsoft Windows 10	Virtualizado
Dominios EMAPA	Servidor	192.168.24.23	Microsoft Windows Server 2012 Standard	Virtualizado
Aplicaciones	Servidor	192.168.24.9	Microsoft Windows Server 2008	Virtualizado

			R2 Standard Service Pack 1	
Licencias ZWCAD	Servidor	192.168.24.12	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Virtualizado
Antivirus	Servidor	192.168.24.7	Microsoft Windows Server 2012 Datacenter	Virtualizado
Registro de Asistencia	Servidor	192.168.24.66	Microsoft Windows Server 2012 Standard	Virtualizado
Desarrollo	Servidor	192.168.24.92	Linux Kernel 2.6	Virtualizado
Cliente GIS EMAPA	Servidor	192.168.24.90	Linux Kernel 2.6	Virtualizado
Help Desk	Servidor	192.168.24.100	Linux Kernel 2.6	Virtualizado
BD Servicios en Línea	Servidor	192.168.24.6	Microsoft Windows	Virtualizado

			Server 2008 R2 Standard	
Financiero Antiguo	Servidor	192.168.24.11	Microsoft Windows Server 2008 R2 Standard Service Pack 1	Virtualizado
Comercial Antiguo	Servidor	192.168.24.3	Microsoft Windows Server 2008 R2 Enterprise	Virtualizado
Documental Antiguo	Servidor	192.168.24.10	Microsoft Windows Server 2003 Service Pack 1	Virtualizado

3.2.2 Selección de la herramienta de análisis de seguridad informática

Para llevar a cabo un análisis exhaustivo de la seguridad informática en los servidores internos de EMAPA, se han seleccionado tres herramientas complementarias: Nessus, Nmap y OpenVAS. Estas herramientas permiten realizar una evaluación integral de vulnerabilidades, mapeo de red y escaneo de servicios, aspectos clave para identificar riesgos potenciales en los sistemas virtualizados de la organización.

Nessus

Nessus, desarrollado por Tenable, es una de las herramientas de escaneo de vulnerabilidades más reconocidas a nivel mundial. Ofrece una amplia cobertura de vulnerabilidades, con más de 88,000 CVEs identificadas y una biblioteca de más de 210,000 plugins que se actualizan en tiempo real. Nessus proporciona más de 450

plantillas preconfiguradas para facilitar la identificación y remediación de vulnerabilidades en diversos entornos, incluyendo sistemas operativos, dispositivos de red y aplicaciones. Su interfaz intuitiva y sus capacidades de generación de informes detallados permiten a los equipos de seguridad priorizar eficazmente las acciones correctivas [29].

Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada principalmente para el descubrimiento de hosts y servicios en una red. Es ideal para realizar un inventario inicial de dispositivos conectados, identificar puertos abiertos y determinar los sistemas operativos en uso. Nmap emplea paquetes IP en formas novedosas para detectar hosts disponibles, servicios ofrecidos, sistemas operativos y otros atributos de la red [31].

OpenVas

OpenVAS (Open Vulnerability Assessment Scanner) es una solución de código abierto para la detección de vulnerabilidades, desarrollada por Greenbone. Ofrece capacidades de escaneo autenticado y no autenticado, soporta diversos protocolos y permite ajustes de rendimiento para escaneos a gran escala. OpenVAS se actualiza diariamente mediante un feed que proporciona pruebas para detectar nuevas vulnerabilidades, lo que garantiza una evaluación continua y actualizada de la seguridad [32].

La combinación de estas herramientas permite realizar un análisis más robusto y completo, abarcando desde la enumeración de dispositivos en red hasta la identificación detallada de vulnerabilidades, mejorando así la precisión en la evaluación de la seguridad informática de los servidores de EMAPA [33].

3.2.3 Análisis de las vulnerabilidades en los servidores internos de EMAPA

3.2.3.1 Servidor 1 de Correo

En la presente Figura 1, se visualiza sobre el servidor Intranet, donde hace referencia que se encuentra la respectiva cantidad de vulnerabilidades en las que se distribuyen en 0 Critical, 1 High, 28 Medium y 2 Low, de tal forma que tambien se especifica el sistema operativo Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8

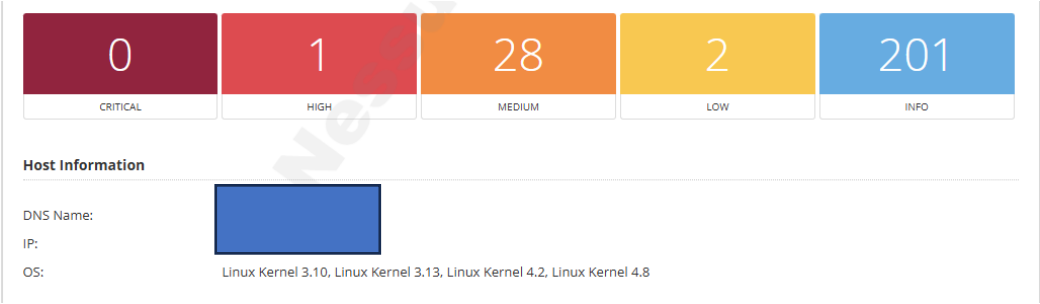


Figura 13. Resultado escanéo Servidor 1 de Correo

- **42873 – SSL Medium Sstrength Cipher Suites Supported (SWEET32)**

Mediante el reporte con la herramienta Nessus utilizada, genera una solución de remediación adecuada sobre el impacto de la vulnerabilidad en el servidor presente.

A continuación se logra mostra los detalles de cada uno de las vulnerabilidades más específicas en el Servidor de Correo:



Identificación

Mediante la herramienta de Nessus se logró detectar que tiene habilitado un cifrado simétrico de una fortaleza media, con la que específicamente se encuentra en el puerto 10000. Esta presente configuración relativamente se encuentra asociada con la vulnerabilidad conocida como WEET32, en donde recibe un ataque de manera criptográfica que se base principalmente en colisiones al momento de utilizar cifrados EDES en ciertas conexiones largas.

Evaluación del Riesgo

Esta presente vulnerabilidad tiene evaluación de los CVSS v3.0 con una puntuación alta de 7.5, en el caso del CVSS v2.0 tiene un puntaje de 5.0 y se considera alta.

Finalmente, el promedio de la explotación masiva es de 0.0398, a medida que estos datos fueron obtenidos desde la herramienta mediante el escaneo del servidor de correo se eviten el siguiente impacto:

Impacto:

- **Confidencialidad:** Alta
- **Integridad:** No se encuentra afectadas
- **Tipo de ataque:** Ejecución de manera remota

Remediación

La presente remediación para una mitigación es reconfigurar el servicio mediante el puerto 10000 en la que se deshabilita ciertos cifrados con una fortaleza media, tomando en cuenta integración de 3DES.

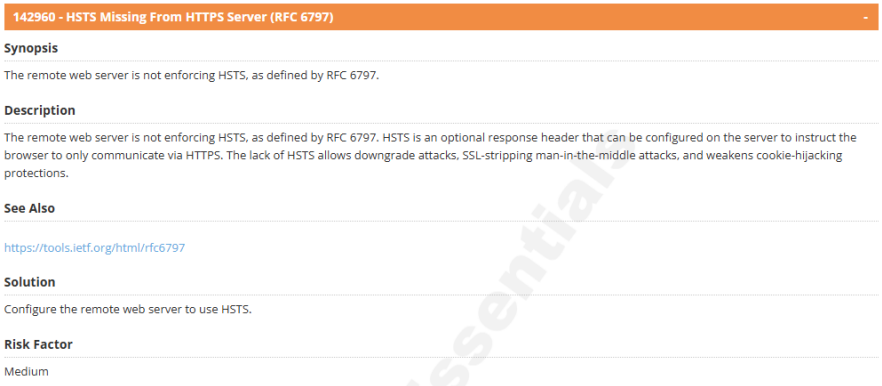
Analisis de resultados

El impacto que representa esta vulnerabilidad específicamente no tiene una acción inmediata, donde relativamente la presencia de 3DES permite que los respectivos atacantes tienen el acceso a ejecutar una captura para poder descifrar ciertas sesiones donde se comprometen los servicios administrativos de manera interna en la que se encuentran en ese puerto.

Además, requiere condiciones específicas para que sea un poco más efectiva, tomando en cuenta su existencia que la red corporativa de la organización empresarial se genera

una postura más debilitante para la seguridad en general ya que si existen una explotación de la presente vulnerabilidad sobre el puerto un personal atacante logra tener acceso a la red local.

- **142960 – HSTS Mising From HTTPS Server (RFC 6797)**



Identificación

Mediante el presente escaneo esta vulnerabilidad que el servidor web logra operar sobre el puerto 443 considerado como HTTPS, no tiene prácticamente habilitado el encabezado denominado como Strict-Transport-Security, donde específicamente se fundamentó como una vulnerabilidad registrada por omisión con el fin de que el servidor se quede sin fuerza del uso exclusivo de HTTPS en ciertas sesiones iniciadas desde un navegador ejecutado con la conectividad hacia internet.

Principalmente uno de los factores consecuentes es que tiene el factor posible en realizar un ataque de tipo dowgrade, en la que generalmente ciertos usuarios permiten que sea ejecutando una redirección hacia la conectividad de HTTP, en la que se identifica como no cifrada, toando en cuenta que el acceso tiene hacia la cierta modificación del tráfico entre cliente y servidor especifico.

Evaluación del Riesgo

Esta vulnerabilidad previamente tiene la clasificación de ciertos factores de riesgo, tomando en cuenta que corresponde las siguientes métricas de CVSS v3.0 con un promedio del 6,5 y el CVSS v2.0 con un total de 5,8.

De tal manera que le tipo de vulnerabilidad se define como una defectuosa ejecución de la configuración dentro del servidor web en la que corresponde con nivel de

aplicación adecuada, por otro lado, el tipo de ataque se genera de manera remota ya que se acude sin requerimiento por medio de una autenticación.

Impacto

Confidencialidad: Procede en identificar las interceptaciones del tráfico de la red.

Integridad: Acoge con un riesgo que manipula el tráfico.

Disponibilidad: No es afectada de manera directa.

Previamente en el entorno corporativos de la empresa EMAPA

Remediación

Es necesario utilizar la configuración de un servidor remoto por medio de una plataforma web, donde se usa un protocolo HSTS.

Análisis de resultados

A lo largo de esta vulnerabilidad tiene la posibilidad en la que tiene una respuesta original, donde indica que el navegador es comunicado por medio de un servicio en HTTPS, en la que logra permitir ciertos ataques de la degradación en ciertas protecciones hacia las cookies respectivas.

3.2.3.2 Servidor 2 SGBD Documental

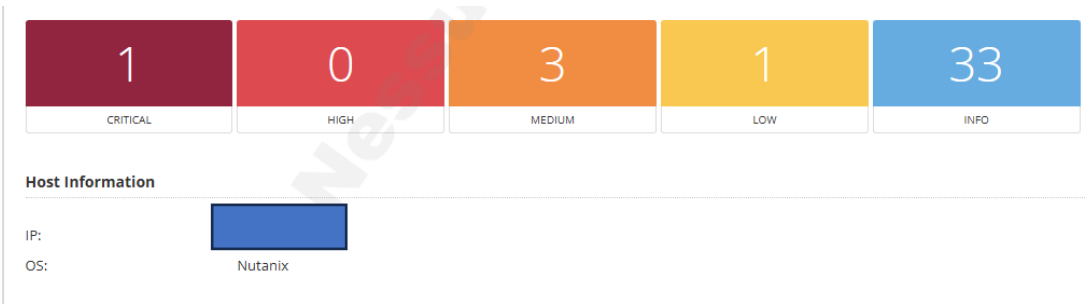


Figura 14. Resultado Servidor 2 SGBD Documental

- **55786 - Oracle Database Unsupported Version Detection**

Identificación

Mediante el escaneo respectivo basado en el servidor en SGB Documental se considera de una vulnerabilidad crítica en la que el servicio de la base de datos esta ejecutada en Oracle, donde relativamente está expuesta por el puerto 1521, priorizada la funcionalidad con la versión 12.2.0.10, la cual logra demostrar que se encuentra fuera del bucle enfocado en el soporte oficial por parte del proveedor.

Evaluación de Riesgo

A lo largo de esta respectiva evaluación se base principalmente en el análisis de CVSS v.0 Base con un resultado promedio total de 10,0 en la que se considera como un riesgo crítico a que posee un vector de ataque en la parte externa de la red preconfigurada, y, por otra parte, no se requiere autenticación.

Impacto

Confidencialidad: Se trata de traer una comprensión en los respectivos riesgos de acceso hacia los datos del servicio ejecutado.

Integridad: Este proceso tiene el objetivo de tener un riesgo para la manipulación de los datos.

Disponibilidad: Generalmente es enfocada en un riesgo de la denegación de ciertos servicios mediante la caída del sistema adecuado del acceso y ejecución hacia la base de datos de Oracle por los usuarios que priorizan el ingreso.

Uno de los análisis que genera mayor impacto crítico es por el uso obsoleto del servicio de la base de datos denominada como Oracle Database en la que se compromete con los procesos consideradas como: Los sistemas de gestión de usuarios, clientes y facturación, Interfaces de acceso para analizar los datos en la institución corporativa, gestión de repositorios de una información crítica juntamente con el proceso de transacciones.

Finalmente, tiene las consecuencias organizacionales en la que se derivan mediante documentación de exploit considerados como públicos y automatizados, en la que se

puede generar filtraciones de acceso de otros usuarios con hacia los datos de manera sensible considerandos como ataques de ciberseguridad informática.

Remediación

La solución de remediación es actualizar a una versión estable de Oracle Database 19c o 21c, en la que se pude realizar una planificación con una versión estable con mayor soporte, a su vez verificar su compatibilidad de ciertas aplicaciones en la que tiene funcionales dentro de la organización empresarial y finalmente realizar una documentación para la migración de los datos a la nueva versión tomando en cuenta que se genera un nuevo proceso de las pruebas dentro del entorno ejecutable.

Mitigación

- Contribuir en la restricción del acceso al puerto 1521 en las direcciones de red no autorizadas.
- Configurar ciertas reglas de firewalls para el segmento de la red
- Realizar un monitoreo para observar el tráfico de la red para detectar ciertas ejecuciones para las explotaciones de patrones de acceso.
- Tener en cuenta la revisión de las auditorias del acceso y configuraciones hacia el motor de la base de datos.
- Generar un control de los roles o privilegios de usuarios hacia el acceso del servicio de Oracle Database.

Análisis de resultados

Generalmente la presencia de esta vulnerabilidad específica se considera un enfoque débil en la infraestructura informática del servidor de EMAPA, ya que reduce la capacidad ante las nuevas amenazas que se presenten, también logra aumentar cierta probabilidad de una mayor interrupción en los servicios que se ejecutan dentro de la organización empresarial, finalmente tiene la postura débil de la seguridad de los datos en la institución.

El impacto directo que contribuye a una disponibilidad de los servicios de la base de datos a un ataque de mayor prioridad, juntamente con ciertas filtraciones de los datos institucionales y para finalizar una determinada dificultad para continuar con la gestión

operativa dentro de la organización empresarial ante los incidentes de la seguridad informática de la base de datos.

- **51192 - SSL Certificate Cannot Be Trusted**

Identificación

Mediante la presente identificación esta vulnerabilidad se logra detectar mediante un servicio web en la que eventualmente es expuesto por medio del puerto 8443, donde consiste en presentar un certificado considerado como SSL considera no confiable para la organización, lo cual se implementa una respectiva cadena de alta confianza. A lo largo de esta certificación en el presente servidor se encuentra auto firmado por el mismo autor en la que ejecuto por el mismo autor.

Donde se descifran doce tipos:

Subject: CN=klever lascano

Issuer: CN=klever lascano

Específicamente esta certificación del SSL tine una fecha emitida desde el 22 de mayo del año 2016, donde por lógica de visualización ya no es considerada válido.

Evaluación del riesgo

En el caso de CVSS v3.0 se deriva con promedio de 6.5 en la que se considera como riesgo medio, pero en el caso del CVSS v2.0 tiene un promedio de 6.4, donde generalmente existe las condiciones necesarias para trabajar en un ataque, en la que se constituye en lo siguiente: No es tiene requerimientos para una autenticación previa, tiene un acceso de forma remota y finalmente tiene un alto potencial para suplantar la identidad considerada como MITM.

Impacto

Confidencialidad: Generalmente esto constituye en los datos tiene el objetivo de ser interceptados.

Integridad: Obtiene la posibilidad de tener una alteración de comunicaciones exclusivas para su funcionalidad del certificado.

Disponibilidad: Específicamente no se observa con una mayor afectación.

Remediación

Al obtener un certificado emitida de manera digital contribuye en ser reconocida de una organización o contrato del dominio configurado de un alto porcentaje de certificación, donde se logra asegurar que incluya la respectiva cadena de validación para complementar una configuración previa del servidor para certificados intermedios y aportar funcionamiento del servidor sobre esta vulnerabilidad identificada.

Mitigación

En la empresa EMAPA debería implementar una política institucional donde se beneficia de un ciclo de vida por parte de los certificados hasta una fecha límite que generalmente incluya:

- El monitoreo antes que llegue la fecha límite para una nueva renovación del certificado.
- Ejecutar un registro de todos los certificados que se encuentran configurados en cada uno de los servidores internos.
- Tener en cuenta la asignación del personal adecuado para el gestionamiento de una identidad de la certificación de manera digital.

En el caso de la correcta configuración de los certificados es importante recalcar que también es necesario reconfigurar todos los servicios conocidos que utilicen el HTTPS teniendo en cuenta que debe estar netamente configurado por el puerto 8443 para tener la ventaja de habilitar ciertos protocolos de forma segura con TLS de 1.2 o superiores.

Finalmente, al considerar una renovación y una nueva configuración implementado en los presentes servidores o varios servidores de la organización empresarial, debe tener en cuenta el objetivo de capacitar al personal técnico sobre ciertos riesgos que existen de los certificados auto firmados dentro de los entornos productivos.

Análisis de resultados

Esta vulnerabilidad tiene el objetivo en generar ciertos servicios que ofrece la empresa EMAPA, donde por medio de las sus plataformas web e internas o externas tiene los principales riesgos que se consideran como vulnerabilidades ante los ataques de intermediarios, obtener una falsa identificación de la seguridad dentro de cada uno de los servicios y finalmente no tiene confiabilidad con los navegadores modernos, ya

que generalmente se obtendrá un resultado deficiente juntamente con alertas en ciertos procesos operativo.

El impacto dentro de organización empresarial es que puede tener una gran pérdida de los servicios de cada uno de los dominio o páginas web que utilizan dentro de cada departamento de manera interna o externa mediante la ejecución de los sistemas web, n la que con lleva en manejar datos relativamente sensibles para la afectación de una operatividad continua mediante navegadores, herramientas de un monitoreo automatizado.

- **57582 - SSL Self-Signed Certificate**

Identificación

Durante el proceso de análisis de seguridad informática en los servicios web internos, se identificó la vulnerabilidad correspondiente al uso de un certificado SSL auto-firmado, detectado en el puerto 8443 del servidor. Este tipo de certificado no está respaldado por una autoridad certificadora reconocida, lo que genera una ruptura en la cadena de confianza establecida para entornos productivos. Específicamente, el certificado examinado presenta la siguiente información:

CN=klever lascano

Evaluación del riesgo

Según la escala del Common Vulnerability Scoring System (CVSS), esta vulnerabilidad presenta un riesgo medio, con una puntuación de 6.5 en CVSS v3.0 y 6.4 en CVSS v2.0. Su nivel de criticidad se debe a las siguientes condiciones:

- No requiere autenticación previa.
- Permite el acceso remoto al servicio afectado.
- Existe un alto riesgo de suplantación de identidad mediante ataques tipo Man-in-the-Middle (MITM).

Esto genera un escenario favorable para que actores maliciosos intercepten o manipulen las comunicaciones sin ser detectados fácilmente.

Impacto

Confidencialidad: Se ve comprometida debido a la posibilidad de que terceros intercepten datos transmitidos entre el cliente y el servidor.

Integridad: La información intercambiada podría ser alterada sin que las partes legítimas lo adviertan.

Disponibilidad: Aunque no se ve directamente afectada en este caso, la desconfianza del navegador podría limitar el acceso al servicio.

Remediación

La solución principal consiste en reemplazar el certificado SSL auto firmado por uno emitido por una autoridad certificadora (CA) confiable. Este nuevo certificado debe cumplir con los estándares internacionales de seguridad y debe incluir una cadena de certificados intermedios correctamente configurada. Asimismo, es esencial asegurar que la nueva configuración sea desplegada en el servidor correspondiente y que se valide su funcionamiento mediante herramientas de monitoreo SSL.

Mitigación

Para reducir el riesgo de recurrencia, se recomienda a la empresa EMAPA implementar una política institucional de gestión del ciclo de vida de los certificados digitales. Dicha política debería contemplar:

- Monitoreo proactivo de fechas de expiración de certificados.
- Inventario actualizado de los certificados instalados en cada servidor.
- Asignación de responsabilidades específicas al personal de TI para la gestión segura de la infraestructura de claves públicas (PKI).

Además, se sugiere la reconfiguración de todos los servicios que empleen HTTPS sobre el puerto 8443, asegurando la compatibilidad con versiones seguras de los protocolos TLS 1.2 o superiores. La correcta implementación técnica debe ir acompañada de la capacitación del personal encargado, con el fin de evitar la persistencia de malas prácticas como el uso de certificados auto firmados en entornos productivos.

Análisis de los resultados

La persistencia de certificados auto firmados en sistemas en producción representa una amenaza directa a los servicios web que utiliza la empresa EMAPA. Esta condición puede facilitar ataques de suplantación de identidad, generar alertas de seguridad en los navegadores modernos y disminuir la confianza de los usuarios al acceder a las plataformas institucionales. Además, compromete procesos críticos que manejan información sensible, afectando tanto la operatividad como la imagen corporativa.

El impacto se refleja en posibles interrupciones de los sistemas web internos, problemas en la interoperabilidad con herramientas de monitoreo automático y una exposición innecesaria a riesgos evitables, lo cual contradice las buenas prácticas en ciberseguridad establecidas por estándares internacionales.

3.2.3.3 Servidor 3 Comercial

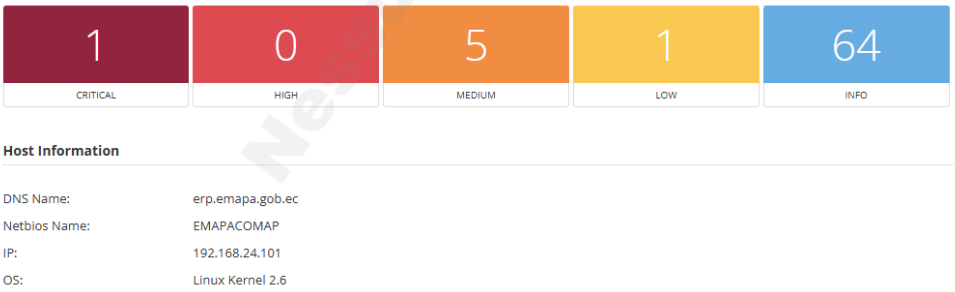


Figura 15. Resultado Servidor 3 Comercial

- **148367 - Python Unsupported Version Detection**

Identificación

Durante el servicio que se ha detectado se encuentra por medio del puerto TCP 5000, donde relativamente se está utilizando la versión de Python de 3.8.2, donde su límite de soporte tiene su finalidad hasta el 14 de octubre de 2024. Generalmente en la versión que se encuentra actualmente por medio del equipo oficial de la herramienta de Python no admiten ciertas seguridades generales en la que es más difícil auditar, para mantener una garantía en el entorno de ejecución.

Evaluación del riesgo

Esto generalmente es apropiado donde se centra un riesgo de nivel crítico para satisfacer el impacto del sistema actual que se encuentra dentro del servidor interno con CVSS v3.0 y v2.0 en la que se obtuvo por medio de la herramienta Nessus con un promedio de 10.0.

Impacto

Confidencialidad: Se considera alta mediante posibles filtraciones ante información relativamente sensible.

Integridad: Modifica una inyección maliciosa en la que se deriva como nivel alto.

Disponibilidad: Tiene la posibilidad de realizar la causa de una caída en el servicio presente por cada explotación de vulnerabilidades.

Remediación

Dentro del ámbito organizacional sobre esta vulnerabilidad, es importante asegurar los sistemas de actualizaciones sobre posibles ataques cibernéticos, y a medida que pasa el tiempo por una gestión de las actualizaciones, para fortalecer una determinada postura de seguridad organizacional utilizando una metodología apropiada, tomando en cuenta que se acople y se adapte acorde la infraestructura tecnológica.

Mitigación

En el caso de tener limitaciones técnicas, permite asegurar dentro de un entorno en la que se encuentra aislado por medio una red pública, donde generalmente se encuentra la aplicación de las reglas de firewalls con accesos que implica restricción, con el objetivo de implementar una limitación de los permisos hacia la ejecución que tiene Python para reducir ciertas limitaciones para reducir el impacto.

Análisis de resultados

Generalmente se encuentra configurado y funcionando en el puerto 5000, donde logra asociar un desarrollo para gestionar aplicativos internos, para que técnicamente disminuya el riesgo hacia la exposición de los datos sensibles que contiene la organización empresarial, donde se compromete para la cierta continuidad de la

operatividad e integridad en diversas áreas del sistema clave para la funcionalidad del servicio.

- **57608 - SMB Signing not required**

Identificación

Generalmente esto se ha identificado considerado como un servidor comercial en la que refleja que se encuentra configurado en el puerto 445, donde prácticamente no tiene habilitada una firma obligatoria por medio de los mensajes de las diferentes conexiones de SMB que ejecutan sin la verificación absoluta aplicando criptografía con integridad y autenticidad de los mensajes. Con la finalidad de formar parte de una característica en la seguridad física para proteger contra los ataques de intermediario y las ejecuciones de comunicaciones entre cliente y servidor.

Remediación

Una de las remediciones importante establece la firma SMB es en base a las verificaciones criptográficas, tomando en cuenta la obligación de garantizar los respectivos paquetes que no se modificaron durante la conexión y la transmisión, donde emite la reducción de cada riesgo mediante los ataques de cierta suplantación y las manipulaciones de cada una de las sesiones inicializadas por cada usuario.

Análisis de resultados

En base al contexto institucional de la empresa EMAPA, el servidor tiene la probabilidad de que ejerza ciertos archivos compartidos que forma parte de algo técnico, respaldos de los sistemas ejecutados en GIS, configuraciones que ejerce la funcionalidad de cada uno de los servicios del agua potable, donde se llegó a la conclusión que por la falta de firma SMB claramente se proyecta en ciertos escalamientos de cierto privilegios donde que genera una propagación en las áreas administrativas y técnicas.

- **51192 - SSL Certificate Cannot Be Trusted**

Identificación

A lo largo del presente servidor expuesto, se da a conocer sobre que da la existencia de un servidor web, donde da a conocer la configuración relativamente insegura para

un certificado SSL/TLS, que generalmente no puede ser confiado por los clientes, con un a mayor cadena de confianza en certificados digitales, en la que emite errores de validez temporal, firma inválida y no confiable, donde prácticamente indica que el certificado no es auto firmado por una CA reconocida.

Remediación

Limitar un acceso al servicio, donde el puerto que se encuentra en el 631, donde da a conocer ciertas reglas en la que el firewalld logra enlistar ciertos controles de acceso e implementas ciertas conexiones remotas por medio de las implementaciones de túneles VPN, en la que genera evitar directamente en un puerto para mitigar en los usuarios para aceptar determinadas advertencias de la seguridad con los certificados no válidos.

Análisis de resultados

La presencia de un certificado no confiable precisamente logra ejecutar la debilitación de la seguridad de la información, por medio de los sistemas que permite restringir ataques MITM, en la que generaliza una cierta desconfianza en recibir sistemas de advertencias hacia el navegador, con la finalidad de permitir una suplantación del servidor actual, donde tiene el objetivo de afectar ciertos procesos críticos bajo los documentos oficiales, actas y respaldos.

3.2.3.4 Servidor 4 BD Comercial

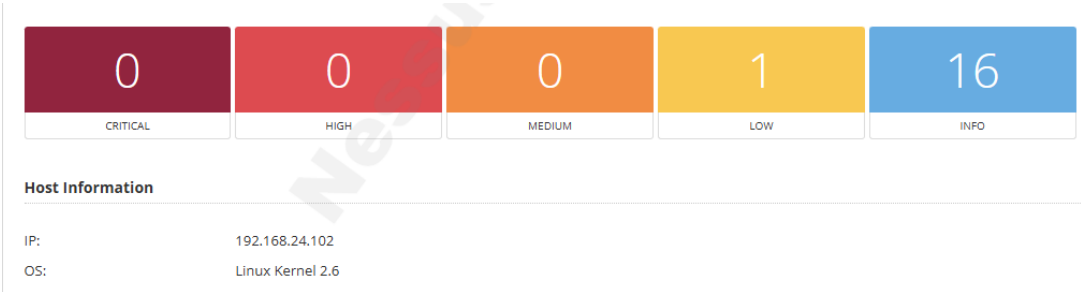


Figura 16. Resultado Servidor 4 BD Comercial

- **10114 - ICMP Timestamp Request Remote Date Disclosure**

Identificación

En este caso se identificó las respectivas solicitudes de ICMP, tomando en cuenta que forma parte del requerimiento de tipo timestamp request, donde logra emitir una

respuesta de tipo 14, donde significa que esto puede admitir por medio de cualquier host de conexión remota, lo cual se cataloga mediante una exposición de cierta información consistente en la que logra representar un acceso de manera directa y una hora exacta para el equipo.

Generalmente esto se logra catalogar por medio de un comportamiento inofensivo, con la sincronización del equipo ya que puede surgir un ataque más inofensivo donde específicamente logran evadir controles de seguridad basados de manera temporal, y representa con un servidor en la que brinda información de manera más precisa.

Evaluación del riesgo

Esta presente vulnerabilidad se considera con un promedio de VPR del 2.2, un EPSS del 0.8939, y se base principalmente en un CVSS v2.0 considerado con un promedio del 2.1, donde se toma en cuenta un bajo impacto de las individualidades para ciertos ataques en la que combina con vulnerabilidades de mayor criticidad.

Impacto

- Confidencialidad: Se da a conocer una exposición de manera parcial al momento de descubrir la configuración del sistema remoto.
- Integridad: Generalmente no logra presenta cierta integridad de los datos
- Disponibilidad: Esto principalmente no logra generar interrupciones ni aspectos que afecta al funcionamiento de cada de los servicios.

Remediación

La solución principal efectivamente consiste en ejecutar un bloqueo de las respectivas solicitudes, donde genera una respuesta de tipo 14 mediante esto genera:

Por medio de una configuración de las reglas en el sistema de firewalld de manera perimetral, esta ejecución se logra utilizar ciertas herramientas utilizadas y conocidas como firewalld, firewalld o ufw, en la que depende por medio de un sistema operativo para descartar ciertos paquetes de mayor atribución.

Para finalizar esta configuración, específicamente surge los sistemas operativos en la que emprende políticas con restricciones del protocolo ICMP si llega el caso de no ser necesario para el funcionamiento de la red en la que se encuentre conectado.

Mitigación

Las consideraciones con medidas complementarias se complementan con una recomendación para verificar en la que ciertos protocolos son asociaos para depender los tipos de mensajes de tipo ICMP, y no llega el caso ejecutar un bloqueo sin ninguna excepción.

Con este punto es importante auditar periódicamente en la que genera una clara seguridad de todos los servidores para ejecutar la identificación de cada una de las exposiciones establecidas por parte del personal de TI.

Finalmente generar una implementación de un segmento de la red para que se establezca la reducción y tenga una visualización de los servicios no muy necesarios externamente.

Análisis de resultados

Uno de los factores de vulnerabilidad se considera por medio un bajo riesgo, donde se toma en cuenta en ciertos entornos críticos con los servidores internos de EMAPA, esto generalmente proporciona una determinada recolección para aborda con la información de un atacante. En este caso genera una respectiva combinación de cada uno de los sistemas que autentica y valida las validaciones de los tokens, mediante un entorno temporal hacia el manejo de procesos relativamente sensibles a sistemas internos, en el caso del monitoreo considerado como SCADA surge varias plataformas web en la que debilitan una postura muy radical, donde omite en una cierta cadena de la defensiva para la infraestructura tecnológica para una mayor organización.

3.2.3.5 Servidor 5 Administrativo

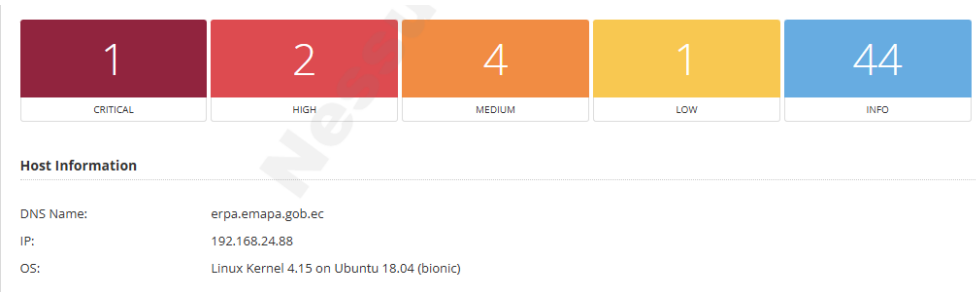


Figura 17. Resultado Servidor 5 Administrativo

- **148367 - Python Unsupported Version Detection**

Identificación

Durante el presente escaneo principalmente se logró detectar un puerto considerado como TCP 5000, en la que efectivamente se encuentra utilizado con una versión anterior para la programación de Python, esto da a conocer que cuya versión específicamente es de 3.8.2 donde brinda un soporte de manera oficial en la que finalizó en la fecha del 4 de octubre del 2024, tomando en cuenta el calendario de las respectivas versiones de Python Software Foundation.

Otro punto importante es que generalmente no logra recibir ciertas actualizaciones de una seguridad adecuada ni juntamente con las correcciones de los errores que presenta en el sistema de las posibles vulnerabilidades, que no so específicamente mitigadas por el proveedor oficial, en la que esta ejecución se encuentra en la ruta principal del sistema operativo analíticamente por el puerto mencionado.

Evaluación de riesgo

Esta vulnerabilidad se presente por medio de un nivel crítico tomando en cuenta ciertas métricas de los formatos CVSS en la que dos de ellas tiene un promedio de 10.00, lo que significa que presenta un nivel de alta criticidad correspondiente a la versión que requiere actualización y en casos posteriores da a conocer fallos explotables con una conectividad remota, sin en el requerimiento de la implementación de las credenciales y a su vez ejecutando un mayor impacto en su totalidad sobre la confidencialidad, integridad y alta disponibilidad del sistema.

Impacto

Confidencialidad: Se considera como una ejecución de alto compromiso mediante le ejecución del código programado, donde no está autorizado, y a medida que pasa el tiempo puede dar acceso a cierta información confidencial de manera sensible que transmite por medio de una aplicativo.

Integridad: En el caso de los riesgos de la manipulación logra generar ciertos datos por medio de un proceso ejecutados dentro del aplicativo web en la que no tiene una versión actualizada.

Disponibilidad: En este caso el funcionamiento del sistema puede definir como inoperativo ya que un respectivo atacante tiene la posibilidad de ejecutar una explotación de datos relativamente vulnerables, en la que llega afectar un servicio que corre el riesgo sobre el puerto 5000.

Remediación

A largo de esta solución específicamente se recomienda en actualizar Python a una versión que actualmente este publicada, con el objetivo de que tambien se obtenga una seguridad de alto consistencia tomando en cuenta la versión de Python 3.10 o superior para llevar a cabo un soporte de mayor actividad y con sus actualizaciones de seguridad.

Mitigación

En este caso la actualización respectiva se debe considerar que no puede realizar la ejecución de ciertas medidas temporales que se define como: Aislamiento de una aplicación dentro de la red segmentada, implementación de las restricciones de un acceso hacia el puerto 5000 limitando que direcciones IPs se encuentran autorizadas.

Finalmente, supervisar el sistema correspondiente si llega a presentarse actividades o intentos de explotación hacia el acceso de IPs descocidas a sistema programado.

Análisis de resultados

Mediante la vulnerabilidad presente se logra identificar como una versión critica de Python, en la que genera una versión de seguridad en los servicios web relativamente desplegados en la organización empresarial de EMAPA, donde forma parte aplicaciones de manera interna hacia un proceso de la gestión operativa para complementar con ciertos casos y servicios críticos, mencionadas anteriormente por el puerto 5000, en la que se requiere una acción inmediata al actualizar Python.

- **35291 - SSL Certificate Signed Using Weak Hashing Algorithm**

Identificación

En este servicio se encuentra identificado por medio de un servicio web de manera activo mediante el puerto TCP 631, en la que es utilizado mediante un algoritmo criptográfico de forma débil considerado como SHA-. En este certificado es

correspondiente a un dominio o entidad en la que específicamente es válido desde el 26 de abril de 2022 hasta la fecha límite establecida hasta el 23 de abril del 20232.

Generalmente el algoritmo SHA-1 se considera que es uno de los más inseguros desde el año 2017, con el objetivo de que existan ciertos tipos de vulnerabilidades mediante ataques de las colisiones, donde su usabilidad se ejecuta una autentificación y alta confiabilidad del canal de cifrado para ejecutar una suplantación del servidor mediante certificados falsificados.

Evaluación del riesgo

En este caso se considera una calificación de riesgo medio ya que es se genera un respaldo con los siguientes puntajes emitidos por un CVSS v3.0 de 7.5 y un CVSS v2.0 con un promedio del 5.0. Finalmente, se tiene el VPR de un promedio total del 4.2, juntamente con el EPSS es 0.0729, en la que compromete de forma integral hacia la conexión SSL, donde la falsificación de identidad de manera digital proviene de una certificación altamente expuestas dentro del presente servidor.

Impacto

Confidencialidad: Se genera un compromiso donde no va directamente por la presente vulnerabilidad, pero queda expuesta de manera continua mediante otras fallas en el descifrado del respectivo canal.

Integridad: En cuestión de esta fase se encuentra altamente afectada ya que el tráfico considerado como HTTPS específicamente se logra suplantar por medio de un certificado de ataque hacia una colisión.

Disponibilidad: No se observa de manera directa el impacto específico en esta vulnerabilidad.

Remediación

La solución principal de esta presente vulnerabilidad consiste generalmente en ejecutar un remplazo del certificado actual, por uno que requiere y utilice un algoritmo de firma con mayor grado de seguridad emitido por la autoridad reconocida como CA, y al menos 2048 bits, que mediante una preferencia el certificado del algoritmo genera como una curva elíptica considera las siglas ECDSA.

Una vez considera esa solución contactar a la emisora para configurar y plasmar el nuevo certificado, solicitar el certificado con el nuevo algoritmo emitido como SHA-2, instalar el presente certificado renovado en el puerto de configuración conocido como 631, y para finalizar reiniciar el servicio para aplicar los respectivos cambios con el servicio SSL.

Mitigación

La compatibilidad del servicio y configuración del certificado no es muy compatible, n la que genera un límite de acceso hacia el puerto 631, donde se considera con redes no confiables en usuarios relativamente autentificados juntamente con la configuración de las reglas del firewall, al momento de reducir los riesgos del tiempo de sesión mediante el uso del servicio de certificación SSL para disminuir una sobreexplotación de SWEET32.

Para concluir esta vulnerabilidad con una mitigación segura y confiable es auditar continuamente el tráfico SSL para implementar la detección de conexiones inusuales o intentos de obtener información dentro del presente servidor.

Análisis de los resultados

A lo largo de esta vulnerabilidad se analiza y se presenta mediante un riesgo de forma silenciosa dentro de los entornos con las comunicaciones que generalmente manipulan los servidores de manera muy constante en diversos sistemas del ERP. En el caso de la organización empresarial EMAPA, generalmente logra facilitar en el método de las ciertas autentificaciones de los servicios internos con la seguridad general en un determinado entrono configurado en la red actual, bajo ciertas condiciones específicas, tomando en cuenta un reemplazo en el uso de los algoritmos y estándares modernos.

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

Identificación

Durante el análisis de seguridad principalmente se encuentra expuesto en el puerto TCP 631, donde se logra soportar como un cifrado SSL, en la que es conocida como Triple DES “3DES”, donde a herramienta Nessus identifico que existe cifrados de bloques hasta de 64 bits que claramente forma parte de un punto clave para efectivizar en los 11e bits de alta vulnerabilidad en los tipos de ataque como SWEET32.

Evaluación de Riesgo

Esta presente vulnerabilidad logra tener en un ámbito de acceso hacia la red para explotar mediante un cifrado con la finalidad de lograr recuperar información para el tráfico cifrado, donde las sesiones son relativamente largas con grandes capacidades de datos con promedio del nivel de riesgo con severidad media en la que se encuentra asociado con CVE-2016-2183.

Impacto

Confidencialidad: Se considera como un grado alto, donde se puede reflejar una determinada cantidad de información intercambiada entre un cliente y un servidor por medio de autenticación o inicios de sesión conocidos como tokens.

Integridad: Específicamente no se ve directamente afectada.

Disponibilidad: No se visualizada con un mayor efecto dentro del servidor

Bajo ciertas condiciones una persona en la que tiene la probabilidad de acceder a la misma red mediante conectividad interna o inalámbrica tiene la facilidad de poner en riesgo la seguridad de la información institucional debido a que captura una gran cantidad de volúmenes del tráfico SSL y TLS.

Remediación

Precisamente debe revisar la configuración donde el servidor en la que se define las configuraciones del servicio SSL, donde prácticamente elimina y deshabilita en menos de 112 bits. Por otro lado, surge la habilitación de cifrados fuertes y modernos llevar a cabo la actualización de una versión en el OpenSSL, donde precisamente reinicia ciertos servicios afectados para aplicar ciertos cambios y con la finalidad de verificar e implementar la nueva configuración de las herramientas como: Nmap juntamente con Openssl.

Mitigación

A lo largo de esta mitigación forma parte de una limitación en el acceso mediante el puerto 631, donde se deriva la configuración con firewalls en dispositivos internos para la reducción en la duración de las sesiones SSL, con la finalidad de capturar suficiente tráfico para explotar SWEET32.

Para finalizar, esto se genera sobre los servicios críticos donde no están expuestos en usuarios o ciertos dispositivos relativamente no autorizados.

Análisis de resultados

A lo largo del impacto de las vulnerabilidades generan procesos que fundamenta una afectación directa en alta disponibilidad del sistema, que representa un alto riesgo de confidencialidad hacia la información que posee la organización empresarial EMAPA.

En la empresa EMAPA se enfoca netamente para ejecutar una gestión de ciertas impresiones o autentificaciones de diversos usuarios donde interceptan ciertos datos para la afectación de una seguridad institucional en las vulnerabilidades de ataques de tipo SWEET32.

- **51192 - SSL Certificate Cannot Be Trusted**

Identificación

A lo largo de este escaneo de seguridad informática se detectó un servicio prácticamente en el puerto TCP 631, donde logra presentar un protocolo SSL no confiable, en la que se considera como una entidad de la siguiente manera:

C=US, CN=erpaplicacion, O=erpaplicacion

Esto significa que logra tratar un certificado con auto firma, donde no es emitido por una autoridad certificadora donde públicamente es reconocida, para romper una cadena de alta confiabilidad.

Remediación

Generalmente para generar una solución es adquirir un certificado del SSL, donde principalmente debe ser confiable y firmado por una autoridad certificadora de alta confiabilidad, posteriormente se logra instalar un nuevo certificado dentro del servidor donde se logra ejecutar un servicio adecuado, para asegurar e incluir una respectiva cadena del servidor, con el objetivo evitar errores hacia la nueva verificación.

Como siguiente punto de remediación, es lograr una verificación para la respectiva implementación del nuevo certificado con herramientas consideradas como Openssl conectada la respectiva Ip del servidor y el puerto ejecutado, tomando en cuenta que

si es accesible por medio de los SSL Labs Server Test. Y para finalizar reiniciar el servicio on los cambios respectivos.

Análisis de los resultados

Mediante el uso de los certificados se considera como auto firmados, donde no son confiables debido a las autenticidades de ciertas conectividades en los protocolos de SSL y TLS. A lo largo del servicio que fundamenta EMAPA se conecta a este servicio que son fundamentales para obtener por medio de un servidor legítimo.

Po otro lado, el funcionamiento del sistema claramente no se ve afectado hacia la percepción de una seguridad por parte del cumplimiento que corresponde a las políticas institucionales de Tecnologías de la Información, donde afectan futuras integraciones en cada uno de los servicios que validan la confiablidad del presente servidor.

- **57582 - SSL Self-Signed Certificate**

Identificación

Mediante el escaneo se detectó un servicio que se encuentra expuesto por medio del puerto TCP 631, en la que se considera con certificado SSL auto firmado donde no se encuentra emitido por una autoridad certificadora, que relativamente se anula la cadena de confianza para que garantice un mejor funcionamiento de autentificación dentro del servidor.

Subjetc:
C=US/CN=erpaplicacion/O=erpaplicacion/OU=Unknown/ST=Unknown/L=Unkonwn

Issuer: Se define como un indicador de forma clara que se encuentra auto firmado.

Remediación

Mediante este proceso se debe adquirir un certificado SSL firmado con una certificadora de alta confiabilidad, en la que se puede utilizar los entornos internos para una CA de manera corporativa de mayor reconocimiento y distribuida en los diversos dispositivos.

A continuación de ese proceso es instalar el certificado SSL donde se encuentra ejecutando el presente servidor y verificar el nuevo certificado utilizando la herramienta Openssl, para tener un acceso optimizado del servicio de internet.

Y para finalizar ejecutar el reinicio del servicio para su implementación y verificación completa, tomando en cuenta la instalación del nuevo certificado para aplicar los cambios respectivos.

Análisis de resultados

La utilizad de los certificados auto firmados se toma en cuenta las políticas básicas que corresponde a la seguridad de la información que utiliza los protocolos SSL y TLS. A lo largo de este procedimiento en la organización de la empresa EMAPA. Generan ciertas advertencias de seguridad en los navegadores de servicios o integraciones que dependen mediante una conexión relativamente segura para llevar a cabo la alta confiabilidad de los usuarios internos con mayor automatización de los sistemas.

Finalmente, al remplazar el certificado por uno que es válido significa tener una seguridad de buenas prácticas en el gestionamiento de los certificados digitales para llevar a cabo una seguridad integra dentro de la infraestructura del departamento de Tecnologías de la Información de la organización empresarial EMAPA.

3.2.3.6 Servidor 6 Dominio SSL EMAPA

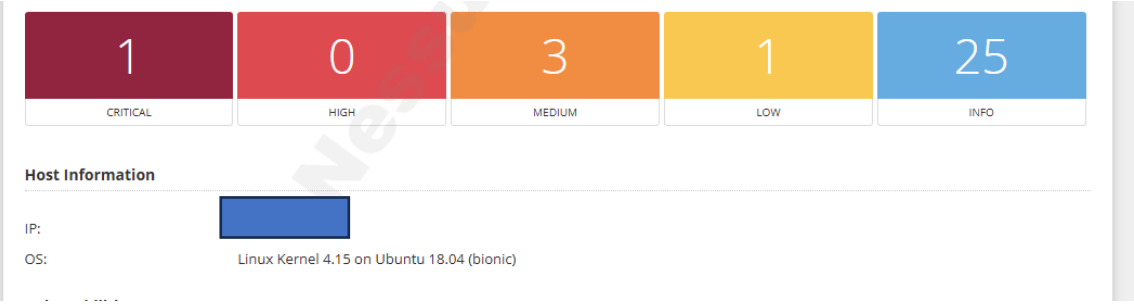


Figura 18. Resultado Servidor 6 Dominicio SSL EMAPA

- **148367 - Python Unsupported Version Detection**

Identificación

A lo largo de este análisis de vulnerabilidades se identifica mediante un servidor que se considera que utiliza el puerto TCP 81, en la que es utilizada mediante una versión de Python de versión desactualizada y específicamente no soportable con: Python 2.7.16.

Generalmente esta versión llegó su ciclo de actualización el 1 de enero del 2020, donde generalmente ya no logra recibir las respectivas actualizaciones de una seguridad ni el mantenimiento de ciertos desarrolladores de manera oficial en el entorno de Python.

Evaluación del riesgo

La respectiva evaluación se da a conocer con un nivel de riesgo crítico, en la que generaliza con CVSS v3 con un total de 10.0 y un CVSS v2 con un promedio de 10.0, ya que representa un máximo control de severidad en la que da la sugerencia de ciertos términos de confidencialidad, integridad y alta disponibilidad.

Impacto

Confidencialidad: En el caso de la herramienta de Python da a conocer ciertas vulnerabilidades, donde generalmente permite tener un acceso no autorizado hacia la información, en la que genera un almacenamiento continuo de mayor sensibilidad junto con un proceso en aplicaciones desarrolladas de su propio entorno.

Integridad: Por la integridad, se ejecuta una alteración del funcionamiento hacia el sistema para modificar ciertos datos ejecutando sin la autorización.

Disponibilidad: Se ejecuta fallos críticos donde se da a conocer que la versión es un fundamento muy importante en los aplicativos webs, ya que el sistema de monitoreo se base principalmente en una API para el consumo de manera interna y externa, donde presenta un riesgo de severidad alta en ciertos procesos críticos que constituye la infraestructura de la organización institucional de la empresa EMAPA.

Remediación

Es recomendable actualizar mediante una versión que logra soportar de la versión estable máximo de 3.10 o superior, por otra parte, es importante verificar una

determinada compatibilidad de ciertas aplicaciones para ejecutar el proceso de la migración.

En el caso de la ejecución de pruebas es importante reflejar diversas pruebas de regresión funcional sobre algunas aplicaciones que depende sobre la herramienta de Python para implementar en ciertos cambios de las producciones, donde aplica con mayor seguridad en el mantenimiento entorno con la actualización mediante el mismo sistema de versiones gestionables.

Mitigación

Es importante ejecutar la actualización de forma inmediata para que el servicio que se encuentre en el puerto 81 es brindar un aislamiento, con la finalidad de restringir el acceso hacia los usuarios que brinden servicios autorizados. Para llevar a cabo el monitoreo de manera continua hacia el tráfico de red, con los diversos registros de los errores y las alertas para detectar varios comportamientos de anomalías riesgosas.

Análisis de los resultados

En el caso de la usabilidad de las versiones desactualizadas son obsoletas ya que los lenguajes de la programación logran representar una falla de la estructura en la gestión de software para satisfacer mayor seguridad en versiones que no complementan las múltiples vulnerabilidades en la que no existen remediaciones disponibles dentro de la organización empresarial EMAPA, en este caso se manejan diversos datos sensibles para una gestión del agua potable, tomando en cuenta los entornos de seguridad apropiada y con una actualización continua dentro del negocio para brindad una alta confianza en los sistemas que maneja a nivel institucional.

Finalmente, al ejecutar la actualización de Python principalmente garantizan une entorno más eficiente, seguro y compatible con los respectivos mantenimientos de los sistemas de mayor utilización dentro de la institución que brinda los servicios dentro del servidor.

- **159490/15490/187201 - OpenSSH < 7.8, 8.0, 9.6 Multiple Vulnerabilities**

Identificación

Mediante el escaneo de la presente vulnerabilidad donde específicamente se identificaron en el servicio SSH visualizado en el puerto TCP 22, en la que se genera una ejecución la versión Open SSH 7.6p1, lo cual se concluye que se encuentra desactualizada, en la que da a conocer en la infraestructura tecnológica con las siguientes amenazas:

CVE-2018-15473 – Vulnerabilidad ID: 1597490

Representa la fuga de la información por diversos paquetes de información en la que se encuentran enumerados por distintos usuarios que se considera válido, con el objetivo que no existan una autenticación de usuarios no válidos.

CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111 – Vulnerabilidad ID: 159491

Estas vulnerabilidades se consideran por un cliente determinado como scp, en la que incluye por medio de las descargas de diversos archivos mediante un servidor defectuoso denominadas como scp.

CVE-2023-48795, CVE-2023-51384, CVE-2023-51385

En el caso de este tipo de vulnerabilidades forma parte de ciertas inyecciones en la que consiste y tiene fallos mediante restricciones claves para determinar y llevar a cabo una explotación avanzada, donde permite ejecutar una manipulación del protocolo SSH para generar ciertas inyecciones juntamente implementando ciertos caracteres especiales para complementar las restricciones de las partes claves de la aplicación dentro del servidor.

Evaluación del riesgo

Se considera con un nivel de criticidad en nivel medio, en la que la fuga del riesgo se evalúa, por medio del compromiso en la integridad del cliente, y mediante un respectivo riesgo de ataque MITM.

Impacto

Confidencialidad: Se filtra una información específica en la que se deriva por medio de metadatos en otros usuarios con mayor validez a través del servidor scp.

Integridad: Generalmente puede transcurrir fallas en el servidor, tomando en cuenta que permite un ataque de la manipulación de mensajes de una fase inicial enfocado al protocolo SSH.

Disponibilidad: Tiene la conclusión en no afectar directamente, para la explotación donde precisamente conduce a la denegación en servicios posteriores con mayor persistencia.

Y llevando dentro del contexto de la organización empresarial de EMAPA, son enfocados en los servicios SSH, onde se utilizan por una conectividad de forma remota para generar una administración en ciertos sistemas críticos de las bases de datos, ERP y los backups de cada uno de los departamentos institucionales, en la que tiene la conclusión de representar un riesgo de mayor relevancia operativa confiable y segura.

Remediación

Actualizar la versión del protocolo OpenSSH a la versión 9.6 o superior, en que enfoca en ejecutar una corrección técnica en todas las vulnerabilidades indicadas.

Para le sistema Ubuntu es necesario ejecutar los siguientes comandos:

sudo apt update

sudo apt install --only-upgrade openssh-server

Donde por medio de ellos se instala y se actualiza el protocolo OpenSSH-Server para un correcto funcionamiento eventualmente virtualizado en el sistema de Ubuntu.

Es necesario revisar las configuraciones del cliente scp, donde se deshabilita o limita a su uso, para aplicar las diversas políticas de un mayor control en versiones posteriores tomando en cuenta las actualizaciones en los servicios de mayor criticidad.

Y para finalizar en este servidor es necesario verificar el estado de la versión actualizada en el siguiente comando en el sistema del servidor:

ssh -V

Mitigación

Obtener una limitación hacia el acceso del SSH mediante ciertas restricciones de las configuraciones del firewalld o las reglas de los iptables, por medio de los usuarios relativamente autorizados.

En este caso es importante implementar una autenticación en la que se conectan los usuarios por medio SSH, y en este ciclo de la ejecución deshabilitar el uso del scp mediante las restricciones que se considera como un registro y auditoría en varios intentos de las conexiones en unan determinada cantidad de los usuarios.

Análisis de resultados

A lo largo de la utilización de la versión de OpenSSH en la empresa EMAPA, relativamente se compromete con ciertos pilares y fundamentos de seguridades enfocados con la seguridad para identificar con los usuarios válidos donde modifica diversos archivos remotamente expuestos en la conexión de los ataques de tipo Man-In-The-Middle “MITM”.

Para finalizar este análisis de la presente vulnerabilidad es genera una actualización de la versión recomendada, donde la mejor postura de seguridad es de forma general para el cumplimiento de la forma práctica de una ciberseguridad más controlada, tal como varios organismos internacionales como NIS y OWASP consideran hacer en los procesos de implementar Seguridad de la Información en instituciones grandes en este caso como es entidad pública de EMAPA.

3.2.3.7 Servidor 7 BD Administrativo EMAPA

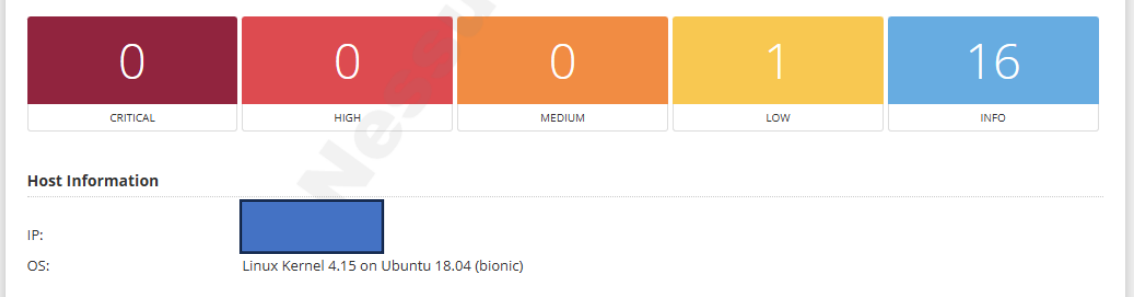


Figura 19. Resultado Servidor 7 BD Administrativo EMAPA

- **10114 - ICMP Timestamp Request Remote Date Disclosure**

Identificación

Se genera una detección del sistema objetivo donde relativamente responde a las solicitudes con el protocolo ICMP considerado como timestap de tipo 13 y 14, en a que permite que un usuario se conecta remotamente para determinar una hora exacta, tomando en cuenta el equipo local donde se encuentra con un respectivo objetivo que se encuentra en e puerto 0 de puerto identificado anteriormente, ya que el reloj remoto se sincroniza de forma local en el equipo respectivo.

Remediación

En el caso de las solicitudes ICMP, se toma en cuenta en aplicar las políticas de un control de tráfico de alta complejidad con paquetes de tipo 13 y 14, pero remediar ciertas fases Complexivo se define de la siguiente manera:

Configuración de las políticas del firewall para vengar un tráfico de red

Desactivar el servicio del protocolo ICMP

Implementar ciertas listas de un control de acceso con las reglas de ACLs para recibir solicitudes de manera externa al ejecutar la conectividad hacia el servidor.

Análisis de resultados

Mediante la entidad e la organización de la empresa EMAPA, la presente vulnerabilidad contribuye como un punto innecesario en la que el host en la conexión de internet logre obtener la hora específica del sistema local, donde refleja ciertas técnicas de identificación del sistema operativo y el comportamiento de la red, ejecución de un mayor control de acceso interno del sistema y finalmente verificar el estado del funcionamiento interno del sistema.

En este caso, dentro de este servidor no existe ninguna funcionalidad crítica ya que únicamente depende del protocolo ICMP, con la finalidad de que no exista ningún bloqueo en los diagnósticos comunes de la red corporativa, en la que se concluye que su mitigación es baja, ya que tiene una remediación optima.

3.2.3.8 Servidor 8 Servicios en línea EMAPA

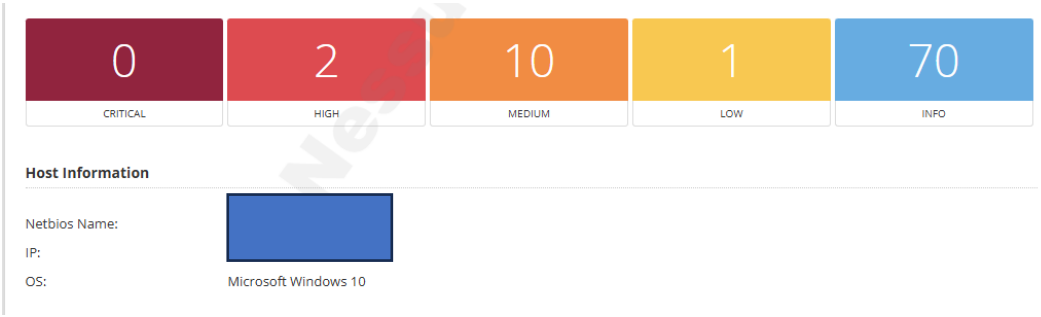


Figura 20. Resultado Servidor 8 Servicios en línea EMAPA

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

Identificación

Mediante este servidor remoto permite utilizar un cifrado SSL, donde genera una fuerte media, en particular por lo que se considera vulnerable en el ataque criptográfico como SWEET32, de tal manera que, el cifrado detectado tiene como SHA-1 hacia el puerto 1433 por el protocolo tcp en la que se encuentra los servicios del SQL Server y en el otro puerto configurado como 3389 para el funcionamiento de la conexión remota por escritorio del equipo local.

Evaluación de riesgos

El nivel de riesgo es considera como nivel medio y previamente con los archivos CVSS v3.0 y v2.0 tiene prácticamente un promedio total del 7.5 y 5.0 para este tipo de vulnerabilidades, lo cual se define como un factor de riesgo muy considerable para tomar medidas preventivas sobre esta vulnerabilidad.

Impacto

En base al impacto que conlleva tener esta vulnerabilidad es tener en cuenta la seguridad informática donde generalmente adjunta la parte confidencial que se considera como alta con el objetivo de descifrar ciertas partes del tráfico de forma exitosa, en segundo paso se logra integrar la afectación directa para su seguridad y para finalizar no requiere tener una disponibilidad no muy afectada.

Remediación

En el caso del algoritmo 3DES principalmente se encuentra basado por un cifrado de los bloques en un instancia de 64b bits, en la que genera una relatividad de la conectividad de mayor prolongación en ciertas sesiones interactivas para implementar como RDP o SQL y cierto volumen de datos cifrados, donde se da a conocer que es una solución eficaz en utilizar RFC 7525 para el uso de los TLS en diversas aplicaciones, ejecutar las configuraciones criptográficas de manera débil para abordar OWASP y finalmente es recomendable eliminar 3DES para los entornos de la producción.

Mitigación

En este caso de la presente vulnerabilidad únicamente se logra restringir un acceso hacia los puertos 3389 y 1433, por direcciones IP confiables, donde realmente se implementa un VPN que generaliza para cifrar un canal específico y al monitorear el tráfico del cifrado muy prolongada hacia posibles intentos de conectividad, donde precisamente logra demostrar una cierta cantidad de los posibles intentos de conectividad con cierta probabilidad de mayor prolongación.

Y para finalizar realizar una actualización de cada una de las versiones de TLS hacia las más recientes en la que considera como la 1.2 o 1.3, donde no permiten intervenir el algoritmo 3DES.

Análisis de resultados

En el entorno empresarial, precisamente las distintas sesiones del servicio RDP como factor administrativo implica en ser utilizadas para una configuración, soporte y el gestionamiento de los servidores, donde las bases de datos críticas en el puerto 1433, generalmente forma parte de una sensible información permitiendo así el cumplimiento de ciertas normativas de la seguridad informática, donde mantiene cifrados inseguros de distintos usuarios en las redes internas.

- **57608 - SMB Signing not required**

Identificación

A lo largo de este análisis depende mucho sobre el servidor remoto donde no requiere una firma digital, de esa manera surge comunicaciones acerca de lo que permite el establecimiento para las respectivas conectividades de una mayor integridad entre el puerto afectado configurado como 445 de Microsoft SMB y en base al servicio surge sobre un bloque del servidor que determina mensajes, en la que altera un requerimiento que posibilita las modificaciones y paquetes de verificación integra.

Remediación

Generalmente por medio del protocolo SMB, logran permitir compartir archivos, impresoras y otras utilidades que son fundamentales dentro de la organización empresarial EMAPA, sin embargo, la versión actual que no contiene una firma digital establecida deja precisamente fuera de los datos a ciertas modificaciones en un tránsito en donde la solución recomendable es:

Realizar una protección la integridad de varios mensajes determinados de protocolo, por otra parte, impedir las modificaciones de un alto riesgo y para finalizar es requerir un refuerzo de autenticación sobre la comunicación en configuraciones de la red interna, por otra parte, tambien se recomienda actualizar las versiones más recientes en la que benefician mejoras de los controles y cifrados con mayor seguridad.

Análisis de resultados

Bajo este análisis se integra la manipulación de diversos usos al ejecutar una configuración de la red interna para el uso respectivo de cada departamento y empleados que forma parte de ella, donde generalmente permite una interceptación de los datos administrativos o financieros de la parte funcional que otorga este servidor de servicios en línea que se puede utilizar por otros usuarios de manera interna o externa.

Y para finalizar este enfoque genera ciertas advertencias donde, fundamenta una cierta seguridad de las auditorías internas o externas para la vulnerabilidad estructural.

- **45411 - SSL Certificate with Wrong Hostname**

Identificación

Específicamente se ha identificado por medio un certificado donde es presentado por un servidor en específico, en la que generalmente no coincide con el nombre del hostname, para interpretar que esto fue afectado en el puerto 1433 por el protocolo tcp identificado como el servicio utilizado denominado como Microsoft SQL Server y generalmente se concluye que el nombre del host al que se ejecuta una conexión genera un error de validación para establecer conectividades seguras por usuarios que tengan la posibilidad en realizar esta actividad.

Remediación

Una de las recomendaciones se deben tener en cuenta que un campo considerado como Common Name CN en la que debe coincidir el nombre de servidor al que un determinando cliente se conecta ejerce una probabilidad de conexiones donde se consideran inseguras, por lo tanto, es importante restringir el acceso al puerto 1433 mediante una red interna de confianza, otro punto de mayor importancia es generar el establecimiento de conectividades usando CN para evitar la falencia del hostname y para finalizar este proceso de configuraciones es habilitar ciertas alertas de monitoreo por varios intentos de conexión.

Análisis de resultados

Bajo el contexto de una institución empresarial de EMAPA, esta vulnerabilidad genera varios problemas de conectividades entre las aplicaciones internas que contiene la organización y tambien hacia la base de datos enlazados como SQL Server.

Por otra parte, existen la desconfianza por medio de la identidad del servidor en la que generalmente afecta la autenticación de ciertos datos que son expuestos con mayor integridad.

Y para concluir este análisis es importante resaltar que genera un cumplimiento de las normativas enfocados hacia la ciberseguridad bajo auditorías externas.

- **57582 - SSL Self-Signed Certificate**

Identificación

Durante el presente escaneo se h detectado que ciertos servicios que tiene la empresa EMAPA utilizan los protocolos de SSL auto firmados en la que generalmente los puertos afectados son el: 1433 y 3389, donde los servicios mencionados son realmente auto firmados, en la que no pertenece sobre una certificadora reconocida como CA de mayor confianza durante entornos de prueba.

Remediación

Bajo este proceso es importante reemplazar los certificados auto firmados con certificaciones válidas en base a los entornos públicos o internos, en este punto es recomendable seguir estos pasos de solución:

En el servidor generar un CSR, solicitar un certificado de alta correspondencia validado por CA, una vez configurado estos pasos instalar el certificado dentro del servicio SQL Server y en RDP para complementar con las conexiones remotas de las sesiones iniciadas por el equipo local.

Y finalmente es importante reiniciar los dos servicios que son reconfigurados para que no contengan esta vulnerabilidad presente, toando en cuenta que exista la validación de los certificados dentro del servidor.

Análisis de resultados

Durante el proceso de escaneo en base al servidor de las aplicaciones en línea se determinó que el uso de los certificados auto firmados específicamente pueden interrumpir las conectividades y sistemas de terceros en las que no benefician a certificados confiables dentro de los sistemas remotos como RDP y esto puede ocasionar un rechazo de conexiones y advertencias de seguridad informático al personal que este a cargo del control y restricciones de uso del servidor que emite en la imagen institucional bajo el cumplimiento normativo.

3.2.3.9 Servidor 9 Dominio EMAPA

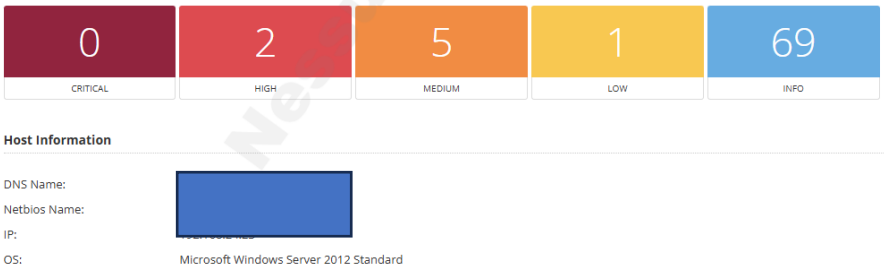


Figura 21. Resultado Servidor 9 Dominio EMAPA

- **35291 - SSL Certificate Signed Using Weak Hashing Algorithm**

Identificación

El respectivo servicio se logró identificar por medio del puerto 3389, en la que se logra utilizar un certificado, donde se genera un algoritmo criptográfico que se considera una debilidad crítica, lo cual se define obsoleto debido a las principales entidades por el tema de la seguridad informática. En el caso del algoritmo SHA-1 principalmente es considerado inseguro, donde permite que un atacante genera ciertos certificados para la suplantación de identidad lo que utilizan este algoritmo como una desaprobación desde el año 2017.

Evaluación del riesgo

En el caso de riesgo s medio, donde los archivos del CVSS v3.0 tiene un promedio del 7.5 y la v2.0 con un total del 5.0, en la que la red pública tiene el objetivo de explotar débilmente para generar un certificado, para suplantar la identidad del servidor, debido a la cadena de confianza para garantizar por medio en el establecimiento de ciertas conexiones por un servidor peligroso.

Impacto

Confidencialidad: Genera un impacto donde o se compromete de manera directa.

Integridad: Se define comprometer el riesgo de suplantación.

Disponibilidad: Verifican la cadena de confianza, en la que principalmente no afecta, su disponibilidad del servidor.

Remediación

Reemitir un nuevo certificado digital, donde actualmente es utilizado por medio de un algoritmo criptográfico como SHA-256, por otro lado, ejecutar una limitación de acceso hacia el puerto 3389, para que las vulnerabilidades documentales no reflejen una colisión altamente crítica y para finalizar imposibilita en garantizar la autenticación al ingresar las credenciales de un usuario específico.

Mitigación

Si llega el caso de no reemitir el certificado actual en preferencia ejecutar una nueva configuración en la que consiste en limitar el acceso hacia el puerto 3389 mediante la aplicación de los firewalls o conexiones VPN, por otra parte, bloquea las determinadas conexiones RDP no autenticadas, con el objetivo de restringir un acceso por la dirección IP para definir de alta confiabilidad sobre el riesgo en utilizar algoritmos débiles en entornos críticos.

Análisis de resultados

A lo largo de este análisis de la respectiva vulnerabilidad generalmente la empresa EMAPA, está vinculado a través de ciertos servicios por parte de la administración remota para el funcionamiento de todos los servicios que se encuentran vinculados, debido al acceso remoto del personal técnico, el gestionamiento de todos los servicios internos de alta criticidad y para finalizar generar una confianza empresarial al no utilizar navegadores seguros por sistemas automatizados.

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

Identificación

Se identifica dentro de este servidor configuraciones de los cifrados conocidos como SSL/TLS, donde especifica el algoritmo 3DES-CBC de un total de 168 bits para considerar ataques criptográficos en sitios inseguros, donde se detecta un servicio defectuoso para que su estructura permite ataques de las respectivas colisiones de los bloques conocidos como el SWEET32 y se detectan en el puerto 3389 por el protocolo tcp, lo cual es insuficiente para proteger grandes volúmenes de datos ejecutados por la transmisión.

Evaluación del riesgo

En base a este riesgo presente se considera como un nivel de riesgo medio, donde prácticamente el promedio de los archivos conocidos como CVSS v3.0 tiene un promedio de 7.5 y la v2.0 con un tota promediado de 5.0.

Impacto

Confidencialidad: Se encuentra con un alto compromiso de los riesgos en la exposición de información.

Integridad: Generalmente no llega afectar dentro de esta vulnerabilidad.

Disponibilidad: No es afectada en el riesgo de la exposición de una determinada información.

Remediación

Este cifrado por el nivel de volúmenes que ofrece la usabilidad de los bloques de 4 bits ya no se considera aceptable por diversos entornos productivos, en medidas de estándares de seguridades con mayor prioridad de modernización, donde se aplica los nuevos reglamentos de los algoritmos criptográficos, la configuración de rechazo hacia los nuevos bloques de los 64 bits, un nuevo uso de 3DES desde el año 2019.

Mitigación

Generar una actualización de la configuración, donde se limita ciertos accesos indebidos por el puerto 3389, tomando en cuenta una administración autorizada, incluir una habilitación VPN donde es eliminando exposición por una directa de la red de internet, minimizar la reducción de ciertas sesiones de RDP en la que se ejecuta una reducción de os ataques SWEET32, para habilitar el protocolo TLS en lugar de tener ejecutado dentro de los servicios las versiones más antiguas.

Análisis de resultados

Bajo el contexto de la empresa EMAPA, este respectivo proceso puede ser utilizado bajo ciertas tareas administrativas con un nivel de mayor criticidad, donde esta respectiva vulnerabilidad puede llegar a tener un mayor impacto negativo, en la que logra trasferir una sensibilidad de múltiples sesiones prolongadas, donde exponen

datos, rompe políticas del cumplimiento y ejecuta una afectación de diversos usuarios técnico.

- **51192 - SSL Certificate Cannot Be Trusted**

Identificación

Mediante el presente servidor presenta remotamente, donde se da a conocer que el certificado se encuentra auto firmado o firmado por una autoridad de la certificación desconocida, lo que impide validar su respectiva autenticidad en la que permite visualizar que el puerto afectado es el 3389 por el protocolo TCP considerado como Microsoft RDP.

A lo largo del escaneo, no puede ser confiablemente validado por una determinada cadena de certificación pública, en la que generalmente tiene posibles causas, en la que se determina una reconocida confianza por ciertos sistemas operativos o navegadores, por las cuestiones de ejecución hacia fechas inválidas del certificado, juntamente con firmas no válidas y desconocidas.

Remediación

Dentro del protocolo SSL se logra basar en la confianza de las autoridades certificadoras, donde generalmente rompe la cadena y no permite ejecutar la validación en la identidad del servidor, donde requiere mecanismos confiables para implementar certificados emitidos por autoridades certificadores con un mayor reconocimiento.

Para remediar este proceso se debe distribuir con un certificado auto firmado dentro de cada uno de los equipos internos en a que se integra la empresa EMAPA, de tal manera que al momento de ejecutar este paso se configura a continuación una restricción de acceso hacia el puerto RDP vía firewalld para monitorear y registrar ciertos accesos del servicio si lega el caso de que existan conexiones sospechosas dentro de la red.

Análisis de resultados

En el entorno de la organización empresarial requiere unas determinadas sesiones en la parte administrativa, donde principalmente adjunta la revisión de ciertas advertencias por la seguridad informática y evitar conectarse mediante cumplimientos

normativos, juntamente con la exposición de los ataques que interceptan las contraseñas hacia los comandos de administración por cada monitoreo ejecutado.

- **65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)**

Identificación

Dentro del servicio RDP el servidor llega a aceptar una determinada aceptación de cada uno de los cifrados de tipo RC4, donde se considera mediante una comunidad criptográficas por ciertos sesgos estadísticos en la que previamente fortalece una vulnerabilidad alta en la parte estructural, donde implica que el atacante logre capturar suficientes transmisiones que parcialmente puede deducir bajo un texto realmente original especialmente por las sesiones de conexiones remotas largas o repetidas.

Remediación

Se ejecuta que el RC4 oficialmente se ha desaprobado donde las vulnerabilidades proporcionan vulnerabilidades criptográficas que generalmente son usas por el entorno interno para considera, donde principalmente se recomienda restringir el acceso hacia el servicio del RDP por firewall en la dirección IP, generar una encapsulación por VPN considerado como un cifrado fuerte y con mayor autenticación, monitorear las conexiones inapropiadas sobre el puerto 3389 y para analizar genera run establecimiento del tiempo de expiración mediante las cortas sesiones de tiempo de conexión hacia el servicio RDP.

Análisis de resultados

En base a este análisis se logra implementar un riesgo de las credenciales hacia la parte administrativa, donde refleja la conexión remota por medio de un cumplimiento con normas internacionales aplicando la seguridad de la ISO 27001.

Y para finalizar genera una exposición prolongada, donde permite ciertos ataques estadísticos con mayor tráfico que intercepta en la parte interna y externa.

- **57582 - SSL Self-Signed Certificate**

Identificación

Se identifica en el puerto 3389 reconocido como Microsoft Remote Desktop Protocol, donde generalmente es utilizado por una cadena inválida de confianza requerida, en la

que se logra autenticar por un servicio, donde diversos clientes cuestionan las advertencias que les presentan en su puerto de trabajo, ya que en eses caso de manera general rechaza la conexión para que obtenga una validación sobre el certificado expuesto.

Remediación

Para ejecutar esta remedición sobre esta vulnerabilidad adquiere en asegurar el acceso del servicio RDP por medio de las redes internas mediante una configuración VPN, como siguiente punto sería en distribuir el certificado en cada uno de los clientes, en la que agrega un certificado la raíz en un soporte de la implementación de los certificados de confianza, monitorear las respectivas conexiones encontradas en el puerto 3389 y para finalizar esta solución de configuración aplicar ciertas políticas en base a una auditoría donde se requiere registrar los acceso dentro del servicio RDP.

Análisis de resultados

En base al contexto institucional ofrece la afectación de ciertos certificados dentro de la confianza en distintos usuarios sobre un servidor que exponen hacia la captura de las credenciales que contiene el servicio RDO y en base a este principio genera ciertos requerimientos con las normativas de la ISO y LOPDO, en donde transmiten los datos personales y sensibles de los procesos críticos dentro del servidor del dominio.

3.2.3.10 Servidor 10 Aplicaciones EMAPA

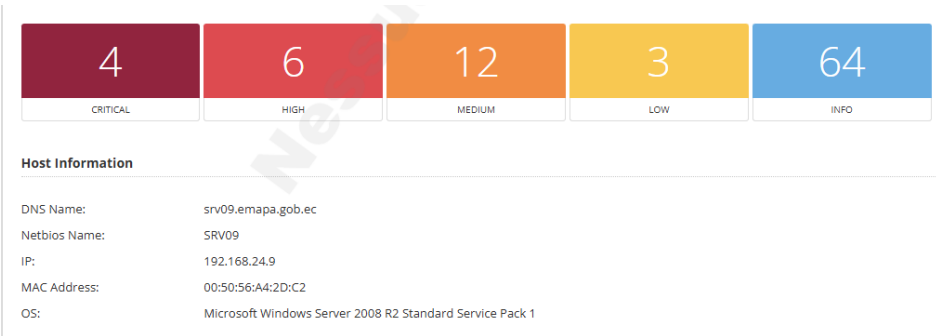


Figura 22. Resultado Servidor 10 Aplicaciones Emapa

- **69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits**

Identificación

Durante el escaneo de seguridad en el puerto TCP/49224, correspondiente a un servicio Microsoft SQL Server expuesto por uno de los servidores internos de EMAPA, se detectó la presencia de un certificado SSL cuyo tamaño de clave RSA es inferior al estándar actual de seguridad.

Específicamente, el certificado identificado como CN=SSL_Self_Signed_Fallback posee una clave RSA de 1024 bits, lo cual no cumple con los requisitos mínimos de seguridad establecidos por el CA/Browser Forum, que desde el 1 de enero de 2014 exige claves de al menos 2048 bits para todos los certificados emitidos.

Remediación

La solución es remplazar todos los certificados con las claves RSA, tomando en cuenta en generar un nuevo par de las claves RSA, donde se fundamenta la utilización de las herramientas de Microsoft y Open SSL, y a su vez emitir con la finalidad de sustituir el certificado con la nueva configuración del servicio.

Análisis de resultados

Aunque esta vulnerabilidad no representa una amenaza directa de explotación inmediata, refleja una mala práctica de configuración de seguridad TLS/SSL. En un entorno empresarial como EMAPA, donde la protección de la información es crítica, el uso de certificados con claves débiles debilita la postura de seguridad global del sistema y puede generar advertencias en navegadores o incompatibilidades con clientes modernos.

- **78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**

Identificación

A lo largo del presente escaneo el análisis de seguridad en el puerto TCP/49224, asociado a un servicio Microsoft SQL Server de la infraestructura de EMAPA, se detectó la presencia de una configuración criptográfica vulnerable conocida como

POODLE (Padding Oracle On Downgraded Legacy Encryption), asociada al uso del protocolo SSLv3 con cifrados en modo CBC (Cipher Block Chaining).

Remediación

Es necesario deshabilitar el soporte de SSLv3, donde tiene que el servicio de Microsoft SQL Server, en la que se define que los servidores son expuestos y es necesario que se requiera atención de soporte temporal lo cual es recomendable habilitar el TSL Fallback SVCSV con cada configuración del presente servidor.

Análisis de resultados

La presencia de esta vulnerabilidad en uno de los servidores de EMAPA demuestra la necesidad de reforzar la configuración de cifrado en los servicios expuestos. Aunque SSLv3 ya es un protocolo obsoleto, su habilitación en los servidores representa una puerta de entrada potencial para atacantes con habilidades intermedias que busquen acceder a información sensible a través de técnicas de degradación de protocolo. La eliminación de este soporte debe considerarse prioritaria para mantener la confidencialidad de las comunicaciones internas y externas.

3.2.3.11 Servidor 11 Licencias WSCAD EMAPA

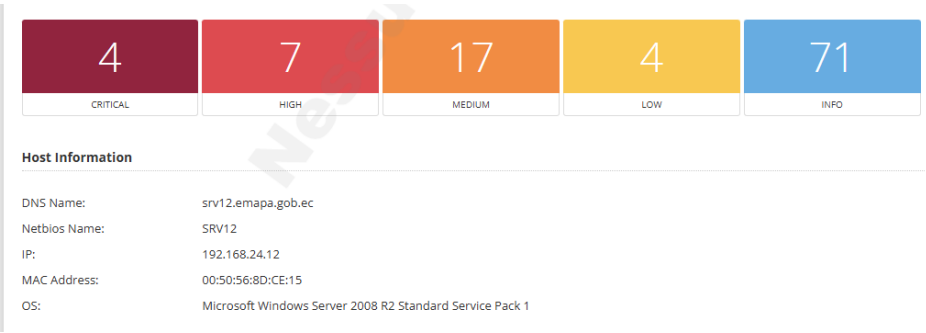


Figura 23. Resultado Servidor 11 Licencias WSCAD EMAPA

En el presente servidor que me refleja la determinada cantidad de vulnerabilidad crítica, alta, media y baja, generalmente da a conocer los mismos riesgos de los anteriores y posteriores análisis de esta fase, con el objetivo de remediar bajo el mismo contexto de remediación al servidor denominado como licencias WSCAD de la organización empresarial EMAPA.

3.2.3.12 Servidor 12 Antivirus EMAPA



Figura 24. Resultado Servidor 12 Antivirus EMAPA

- **79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)**

Identificación

Esta vulnerabilidad se ha detectado mediante el servicio que se encuentra ejecutado RDP, donde uno de los servidores sin expuestos por una vulnerabilidad de manera crítica donde precisamente se asocia por medio del componente Shannel del sistema operativo de Windows, específicamente se encuentra afectado por el puerto 3389, donde un atacante practicante puede tener un acceso remoto no autorizado para generar una explotación en donde tiene la posibilidad de enviar paquetes que se encuentran diseñados para aceptar conexiones TLS, lo que permite ejecutar en e sistema por medio de ciertos privilegios elevados.

Evaluación de riesgo

Este factor se lleva a cabo mediante los archivos CVSS v3.0 en ala que tiene un promedio del 8.8, juntamente con el archivo CVSS v2.0 para complementar con n valor del 10.0.

Impacto

Confidencialidad: Se define como un compromiso completo

Integridad: Establece un compromiso completo

Disponibilidad: Obtiene un compromiso completo de disponibilidad

Remediación

Para ejecutar esta solución es recomendable aplicar de forma inmediata un parche de seguridad del sistema oficial del Microsoft, en la que se logra identificar como KB2992611.

Bajo este proceso de remediación es importante asociar el sistema de riesgo con las normativas relacionadas hacia la aplicación de los sistemas de riesgos, tomando en cuenta la norma ISO/IEC 27001, juntamente con OWAST que generalmente se encuentran en el top 10 para diferenciar la categoría de A05:2021 – Security Misconfiguration.

Mitigación

Generalmente no se logra aplicar un parche donde, no se puede restringir el determinado acceso en el puerto mediante el puerto 3389 en la que las redes IPs genera una administración del firewall. Con la finalidad de establecer una deshabilitación temporal para el uso del Schannel de ciertos servicios en la que no se aplican dentro de la red, de tal manera que implica habilitar una autenticación para diversas capas de protección en factores adicionales, con la finalidad de monitorear el respectivo tráfico por el registro de varios intentos de enfocar la conectividad hacia el servidor del Antivirus.

Análisis de resultados

A lo largo de los procesos críticos precisamente se enfoca en una explotación de la vulnerabilidad, donde genera un código de arbitrarlos por medio del servidor RDP, en la que se compromete con todos los servicios de vario datos alojados. Que pueden considerarse en un factor de riesgo para ejecutar el proceso de gestionamiento hacia el acceso remoto y la administración de los sistemas críticos, donde afecta una mayor continuidad en la operatividad de la organización empresarial EMAPA.

- **35291 - SSL Certificate Signed Using Weak Hashing Algorithm**

Identificación

Principalmente se ha detectado un servicio RDP (Remote Desktop Protocol), donde principalmente se considera un certificado firmado mediante un algoritmo

criptográfico, en la que se beneficia por medio un riesgo de las suplantación de identidad, donde generalmente se encuentra afectado en el puerto 3389, donde la firma ha sido obsoleta desde enero del año 2017, mediante los proveedores de Google Microsoft y Mozilla, en la que representa una grave debilidad criptográfica juntamente con la certificación afectada considerado como un algoritmo tipo SHA-1.

Evaluación del riesgo

En este sobre el nivel de riesgo que emite generalmente es abordado sobre un CVSS de v3.0 con un promedio total del 7.5 y CVSS v2.0 DEL 5.0, principalmente emitido sobre un impacto que genera dentro del funcionamiento de los servicios del servidor.

Impacto

Confidencialidad: Generalmente o es afectado de manera directa.

Integridad: Esto tiene la posibilidad de ser sustituida por el servidor legítimo por un usuario atacante al intentar cambiar las configuraciones de cada uno de los servicios funcionales.

Disponibilidad: Se considera que no puede ser impactada.

Remediación

Mediante esta vulnerabilidad se sugiere ejecutar un remplazo de manera urgente el certificado SSL, con la finalidad que se encuentra firmado con SHA-1, donde debe considerarse que el algoritmo sea más robusto como: SHA-256, y para su funcionalidad es necesario instalar un nuevo certificado con el servidor correspondiente, tomando en cuenta reiniciar el servicio RDP y realizar un escaneo de validación para que tenga la validación y optimizar el registro de esta vulnerabilidad.

Mitigación

Ejecutar una limitación y restricción del acceso hacia el puerto 3389, donde se trata por medio de las redes internas mediante la ejecución y configuración del firewall.

Por otra parte, se da a conocer que se beneficia de una habilitación a nivel de red NLA, tomando en cuenta el servicio RDP, donde generaliza para monitorear ciertas conectividades hacia un registro de los eventos sospechosos.

Y para finalizar es importante deshabilitar los respectivos algoritmos de una configuración mediante una determina política en los registros del sistema de Windows.

Análisis de resultados

La utilización del presente certificado con la firma del algoritmo tipo SHA-1, esto principalmente se logra beneficiar por medio de los servidores legítimos donde es afectado la alta confiabilidad el ejecutar el servicio de escritorio remoto juntamente con otros servicios relativamente cifrados, donde se emplea un riesgo de la integridad en la administración de manera remota hacia el acceso de un personal técnico cumplimiento así la normativa emitida por seguridad de la información aplicando instituciones en la exposición de las sanciones que forma parte la ley y protección de los datos.

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

Identificación

Principalmente esto se ha detectado como un servicio RDP, donde se refleja con los servidores de la empresa EMAPA, en la que se fundamenta que se encuentra configurado por la aceptación de diversas suites en los cifrados SSL, a medida que pasa este proceso es considerado que el cifrado es netamente vulnerable como un ataque SWEET32.

Evaluación de riesgo

Esta evaluación de riesgo se considera como nivel medio ya que se genera un nivel de la métrica mediante que el archivo CVSS v3.0 y v2.0 tiene un promedio del 7.5 y 5.0 para lograr realizar el enfoque analítico para remediar este tipo de vulnerabilidad considera crítico.

Impacto

Confiabilidad: Esto puede ser parcialmente comprometida.

Integridad: No se generar ningún compromiso en la integridad de del riesgo en la vulnerabilidad respectiva.

Disponibilidad: No es comprometida con la disponibilidad especifica.

Remediación

La remediación principal sobre este proceso es en no permitir el uso de los cifrados mediante una fuerza de 3DES, donde generalmente permite priorizar los respectivos algoritmos en la identificación del cifrado SSL tomando en cuenta el servicio RDP identificado como Shanel en el sistema de Windows, la deshabilitación Manuel de pequeños bloques de cifrados, con el objetivo de realizar un forzamiento del uso superior, pero para respectivo requerimiento de funcionamiento es necesario reiniciar los servicios para que aplique los cambios de manera optimizada y adecuada dentro del servidor especifico.

Mitigación

Mediante el caso en no poder aplicar generalmente es importante restringir el respectivo acceso en la que se encuentra el puerto 3389, para que las redes internas se procesa la configuración, por medio de las reglas del firewall, donde es de mayor importancia habilitar una autenticación al nivel de la LAN, para minimizar ciertos riesgos en la captura de las sesiones, con la finalidad de documentar el gestionamiento de los riesgos en cada plazo de la eliminación temporal.

Análisis de resultados

Mediante este tipo de vulnerabilidad es importante interceptar un tráfico de RDP, donde relativamente es importante la red interna para observar la posibilidad de exfiltrar las cookies de las sesiones o credenciales, donde se pone en riesgo de ciertos procesos para la administración remota por cada tipo de sistemas críticos de la empresa EMAPA, donde se fundamenta los servidores de las bases de datos tomando en cuenta la confidencialidad como la seguridad de los datos enfocada en este proceso de análisis.

- **90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)**

Identificación

Mediante esta vulnerabilidad es detectado que uno de los servidores que contiene el sistema Operativo de Windows en la red configurada de la organización empresarial EMAPA, frecuentemente está relativamente expuesto por una vulnerabilidad en la que

es reconocida como Badlock, donde generalmente tiene un protocolo considerado como SAM (Security Account Manager) y LSAD (Local Security Authority Polity).

Este proceso es identificado por los puertos 49155 y 51613, donde el objetivo es forzar una degradación sobre el nivel de la autenticación, posteriormente suplantar a identidad de cada uno de los usuarios mediante el acceso de cada contenido para obtener la información que tiene mayor sensibilidad en las políticas de un dominio de la escala en cada privilegio de la red corporativa.

Remediación

Aplicar la configuración de un sistema de seguridad, en donde se identificado como MS16-047, en la que generalmente es publicado por la página oficial de Microsoft, el cual tiene el objetivo de enfrentar una solución hacia la negociación por medio de los protocolos vulnerables como SAM y LSAD, en la que los diversos sistemas de Windows afectados son los siguientes:

Windows Vista 7, 8.1, 10

Windows Server 2008, 2008 R2, 2012, 2012 R2.

En este caso después del paso primordial mencionado anteriormente es importante, verificar el nivel de cada una de las actualizaciones que forma parte y es ejecutado el sistema operativo.

Por otra parte, es necesario descargar e instalar el KB3148527 en la que forme parte el sistema operativo ejecutado

Y para finalizar es importante reiniciar el sistema configurado para aplicar los cambios de manera satisfactoria nuevamente verificar en un escaneo previo para identificar si la vulnerabilidad que sobresalió no se genera en el registro.

Mitigación

Ejecutar una restricción en el acceso donde los puertos de las redes no son muy confiables, y se requiere implementar la segmentación que se enfatiza por redes VLANs con el objetivo de reducir las posibilidades de los ataques MitM, para aplicar cierta identificación en las comunicaciones entre clientes y servidor,

Finalmente, habilitar y documentar por medio del monitoreo en un tráfico RPC de ciertos comportamientos para establecer la remediación a largo plazo.

Análisis de resultados

En el caso de esta vulnerabilidad en donde los servidores del sistema Windows son fundamentales para tomar en cuenta ciertos roles que pertenece la administración donde autentica y pone en parte los riesgos de cada cuenta, donde la respectiva integridad de los datos es relacionada en cada uno del gestionamiento de cada proceso, recurso, clientes en el sistema de facturación, bajo la configuración de este servidor funcional.

3.2.3.13 Servidor 13 Registros Asistencia EMAPA

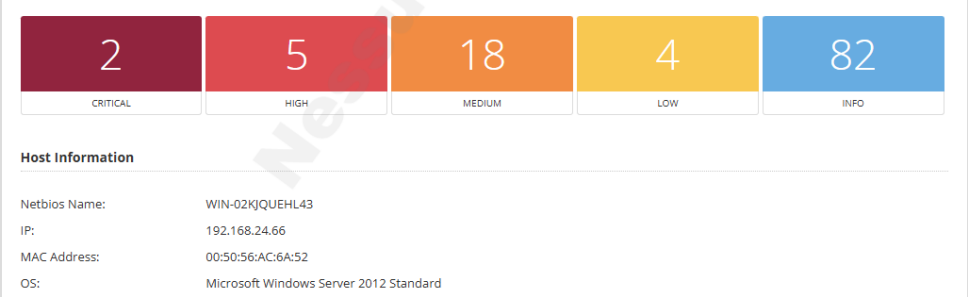


Figura 25. Resultado Servidor 13 Resgistros Asistencias EMAPA

- **73756 - Microsoft SQL Server Unsupported Version Detection (remote check)**

Identificación

Mediante este escaneo es detectado que en el presente servidor considerado como Registros de asistencia forma parte de SQL, de la red donde EMAPA se encuentra ejecutándose hacia una versión absoluta por medio de Microsoft SQL SERVER, en la que se llaga a la finalidad de llegar a un ciclo de vida de soporte.

Por otra parte, el puerto que se encuentra afectado 27934 y específicamente esta versión actual tiene la funcionalidad en la que no recibe actualizaciones de seguridad.

Evaluación del riesgo

Esto en sentido general se considera como nivel de riesgo a un nivel crítico tomando en cuenta las métricas que se maneja son CVSS v3.0 y CVSS v2.0 con un valor promedio al 10.0, en la que se beneficia el riesgo técnico relativamente elevado por la exposición en su totalidad de su mitigación de manera viable.

Impacto

Mediante el suso del respectivo software, donde representa una determinada superficie de mayor significancia por entornos críticos en la que se gestiona en la organización empresarial EMAPA.

Donde este impacto contiene la parte de confidencialidad, integridad y disponibilidad se considera como un grado de impacto alto en los espacios de entorno tecnológico.

Remediación

La principal solución es actualizar de forma inmediata la versión de Microsoft SQL Server a la versión 2019 o 2022, en donde generalmente tiene la facilidad de recibir ciertos parches de seguridad informática por parte del a corporación oficial de Microsoft.

Mediante a este ciclo es necesario identificar las respectivas instancias en a que se identifica por SQL Server con la versión 12.0.2000.0, respaldar de manera completa las bases de datos juntamente con las configuraciones actuales, ejecutar una planificación de la migración hacia una versión soportada para los entornos de pruebas del respectivo servidor.

Finalmente, realizar el enfoque donde se enfoca la aplicación de las buenas prácticas por parte de la instalación en post-seguridad con el propósito de validar el respectivo sistema en la que se encuentra expuesto.

Mitigación

Ejecutar de forma inmediata la restricción del acceso hacia la instancia de SQL Server donde se enfoca únicamente en las direcciones IP de manera interna, donde es necesario implementar un sistema de protección firewall para tener en cuenta la seguridad del sistema operativo y la infraestructura de red, con el propósito que se

ejecute una deshabilitación del acceso del internet juntamente para monitorear las conectividades hacia el puerto 27934 ante accesos no autorizados.

Finalmente, para evitar este tipo de cuestiones es necesario auditar de manera periódica con la finalidad de procesar la detección de los intentos de accesos sospechosos.

Análisis de resultados

Mediante este análisis es primordial identificar ya que las versiones son obsoletas por medio de un riesgo considerable crítico, donde las bases de datos gestionan los usuarios, facturación y los controles en varios recursos hídricos, tomando en cuenta los cumplimientos que surge hacia las normativas técnicas que acoge en base a las reformas regulatorias sobre la disponibilidad operativa para emprender un ataque de manera exitosa con el finde evitar la pérdida o la corrupción de los datos.

- **20007 - SSL Version 2 and 3 Protocol Detection**

Identificación

Esta vulnerabilidad trata sobre conexiones en donde son cifrados servicios donde el servidor dentro la red interna de la empresa EMAPA, genera aceptación de las versiones inseguras por los protocolos SSL de la 2.0 y la 3.0.

Por otra parte, el puerto afectado es el 27934, donde el servicio de Microsoft en SQL Server efectivamente se aceptan conexiones por medio de los cifrados hacia los protocolos en múltiples vulnerabilidades criptográficas, donde puede degradar conexiones TLS a SSL con la finalidad de que pueden negociar versiones más seguras de TLS en los navegadores y aplicaciones mediante un protocolo de negociación hacia las conexiones a versiones inseguras.

Evaluación de riesgo

Generalmente esto se considera como un nivel crítico, tomando en cuenta que la métrica se deriva como CVSS en las versiones v3.0 y v2.0 con los promedios del 9.8 y 10.0, ya que se considera que forma parte de una severidad alta y no cumple un requisito de mayor relevancia en el requisito de la criptografía en las conexiones SSL.

Impacto

Confidencialidad: Se define como una exposición alta de ciertos datos cifrados.

Integridad: Genera una modificación de ciertos riesgos para un tráfico de datos alto.

Disponibilidad: Integra ataques de los potenciales a ciertos servicios críticos.

Remediación

Se recomienda generar una deshabilitación donde el soporte para las SSL tanto de las 2.0 y 3.0 se asegura permitir el uso, en la que es necesario revisar los respectivos archivos de configuración de cada uno de los servidores Apache, Nginx o SQL Server.

Es importante resaltar que es fundamental desactivar las políticas SSL, con el propósito de modificar y actualizar cada una de las versiones que benefician hacia un arreglo de remediación sugerida, y para continuar con este proceso es importante aplicar los parches del software donde el uso no permite deshabilitar por cada una de las configuraciones.

Mitigación

Principalmente es necesario restringir el acceso hacia el puerto donde se conoce como 27934 para tener en cuenta las redes internas con alta confiabilidad, en la que es necesario implementar una VPN con cifrado débiles, en la que conlleva a registrar y monitorear un tráfico SSL para detectar posibles ataques con una negociación insegura, para tener la finalidad de documentar mediante un planteamiento de riesgos de seguridad de la información en la empresa EMAPA.

Análisis de resultados

Mediante el uso de las certificaciones de SSL en dos versiones tanto de la 2.0 como 3.0 es eficaz saber que los servicios de las bases de datos como la herramienta de SQL Server puede ser credenciales hacia los respectivos datos de los clientes y ciertas consultas donde se derivan como la sensibilidad en un tráfico netamente interceptado por un sistema en el cual integra el sistema financiero, privacidad de cada uno de los datos personales, una privacidad corporativa y tomar en cuenta ciertos cumplimientos legales de manera regulatoria por medio de impactos operativos hacia significancias de vulnerabilidades de una nivel de criticidad alta.

- **79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)**

Identificación

Principalmente se ha detectado dentro del servidor de la red configurada por la empresa EMAPA, donde está expuesto por una vulnerabilidad generalmente crítica que genera una afectación hacia un componente que tiene relación hacia el sistema operativo de Windows, principalmente esto contribuye en permitir una vulnerabilidad de conexión remota sin necesidad de autenticar o iniciar sesión hacia el puerto 3389 tcp emitida y conocida como Microsoft Remote Desktop Protocol.

En el caso de este componente tiene el maneja netamente de conexiones seguras donde tiene la desventaja que el manejo de los paquetes de forma incorrecta, lo cual permite realizar que un atacante ejecuta el código arbitrario de forma remota con ciertos privilegios generalmente elevados.

Evaluación del riesgo

Para evaluar el presente nivel de riesgo se genera un nivel crítico, donde se fundamentó por medio dos tipos de archivos como CVSS v3.0 y CVSS v2.0 con un promedio de del 8.8 y 10.0, que genera una alta probabilidad para el impacto en la seguridad de la información.

Impacto

Confidencialidad: Esto genera un impacto considera de forma alta, donde refleja un acceso no autorizado en datos no relevantes.

Integridad: Tiene un riesgo de modificaciones no autorizadas.

Disponibilidad: Posee el riesgo de ejecutar un código de cierta denegación de los servicios.

Remediación

Aplicar de manera inmediata ciertos parches de seguridad por parte del soporte de Microsoft, donde asegura que varios servidores de Windows se encuentran actualizados con una fecha de caducidad hasta noviembre del 2014, con el objetivo

que genere una validación correctamente aplicada mediante las herramientas de escaneo.

Mitigación

Esto generalmente se logra aplicar mediante una restricción hacia el acceso del puerto 3389, por medio de las redes externas que refleja los fundamentos reglamentarios de firewall, donde tiene el mecanismo de habilitar ciertos intrusos con el fin de monitorear el tráfico SSK y TLS, implementar los accesos de los túneles VPN de manera segura.

Análisis de resultados

Esto genera un preciso afecta miento por medio del protocolo de la vulnerabilidad, donde se refleja la utilidad de la administración remota por medio de cada acceso completo del servidor afectado con mayor continuidad operativa en servicios críticos, en la parte de las bases datos financieras, gestión de usuarios en los sistemas internos y para finalizar.

- **35291 - SSL Certificate Signed Using Weak Hashing Algorithm**

Identificación

Principalmente se ha detectado un servicio RDP (Remote Desktop Protocol), donde principalmente se considera un certificado firmado mediante un algoritmo criptográfico, en la que se beneficia por medio un riesgo de las suplantación de identidad, donde generalmente se encuentra afectado en el puerto 3389 y 27934, donde la firma ha sido obsoleta desde el año 2017, donde generalmente este algoritmo es susceptible por medio de los ataques de las colisiones con diferente firma, en la que puede pasar por un servidor afectado hacia la autenticación de la conexión cifrada.

Evaluación del riesgo

En este sobre el nivel de riesgo que emite generalmente es abordado sobre un CVSS de v3.0 con un promedio total del 7.5 y CVSS v2.0 del 5.0, principalmente emitido sobre un impacto que genera dentro del funcionamiento de los servicios del servidor.

Impacto

Confidencialidad: Se ejecuta una suplantación, donde es consideración alta.

Integridad: Esto genera una respectiva manipulación donde es recurrente a proyectar alto riesgo en determinados certificados.

Disponibilidad: Tiene la disponibilidad baja donde se visualiza de manera directa.

Remediación

Mediante esta vulnerabilidad se sugiere ejecutar un remplazo de manera urgente el certificado SSL, con un algoritmo más robusto como: SHA-256, y para su funcionalidad es necesario eliminar los certificados que se encuentran autor firmados para sustituir dentro de un componente débil, al momento de implementar políticas que cumplen ciertos estándares criptográficos.

Mitigación

Ejecutar un remplazo de los certificados con la firma SH-256, donde instala de manera confiable. A medida con las configuraciones es fundamental requerir que los servidores RDP y SQL es necesario actualizar para desactivar los soportes de algoritmos débiles de tipo SHA-1, MD5 dentro de la ejecución del sistema operativo.

Análisis de resultados

La utilización del presente certificado con la firma del algoritmo tipo SHA-1, esto principalmente se logra beneficiar por medio de los servidores legítimos donde es afectado la alta confiabilidad el ejecutar el servicio de escritorio remoto juntamente con el servicio de las bases de datos, donde la autenticación y la integridad se beneficia en ciertos conexones de mayor esencialidad con un acceso no autorizado y acude con la infracción a estándares regulatorios.

- **42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)**

Identificación

Principalmente esto se ha detectado como un servicio RDP, donde se refleja con los servidores de la empresa EMAPA, en la que se fundamenta que se encuentra configurado por la aceptación de diversas suites en los cifrados SSL, a medida que pasa este proceso es considerado que el cifrado es netamente vulnerable como un ataque SWEET32.

Evaluación de riesgo

Esta evaluación de riesgo se considera como nivel medio ya que se genera un nivel de la métrica mediante que el archivo CVSS v3.0 y v2.0 tiene un promedio del 7.5 y 5.0 para lograr realizar el enfoque analítico para remediar este tipo de vulnerabilidad considera crítico.

Impacto

Confiabilidad: Esto puede ser parcialmente comprometida.

Integridad: No se generar ningún compromiso en la integridad de del riesgo en la vulnerabilidad respectiva.

Disponibilidad: No es comprometida con la disponibilidad especifica.

Remediación

La remediación principal sobre este proceso es en no permitir el uso de los cifrados mediante una fuerza de 3DES, donde generalmente permite priorizar los respectivos algoritmos en la identificación del cifrado SSL tomando en cuenta el servicio RDP identificado como Shanel en el sistema de Windows, la deshabilitación Manuel de pequeños bloques de cifrados, con el objetivo de realizar un forzamiento del uso superior, pero para respectivo requerimiento de funcionamiento es necesario reiniciar los servicios para que aplique los cambios de manera optimizada y adecuada dentro del servidor especifico.

Mitigación

Mediante el caso en no poder aplicar generalmente es importante restringir el respectivo acceso en la que se encuentra el puerto 3389, para que las redes internas se procesa la configuración, por medio de las reglas del firewall, donde es de mayor importancia habilitar una autenticación al nivel de la LAN, para minimizar ciertos riesgos en la captura de las sesiones, con la finalidad de documentar el gestionamiento de los riesgos en cada plazo de la eliminación temporal.

Análisis de resultados

Mediante este tipo de vulnerabilidad es importante interceptar un tráfico de RDP, donde relativamente es importante la red interna para observar la posibilidad de

exfiltrar las cookies de las sesiones o credenciales, donde se pone en riesgo de ciertos procesos para la administración remota por cada tipo de sistemas críticos de la empresa EMAPA, donde se fundamenta los servidores de las bases de datos tomando en cuenta la confidencialidad como la seguridad de los datos enfocada en este proceso de análisis.

- **58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only**

Identificación

Esto se encuentra afectado por medio de un servidor dentro de la red interna de la organización empresarial de EMAPA, donde generalmente se encuentra expuesto por la falta de autenticación de nivel de la red NLA, que se ejecuta el servicio de escritorio remoto RDP afectando en el puerto 3389.

Remediación

Generar una habilitación del nivel de autenticación dentro del servidor, donde se debe activar la opción que solo permite conexiones desde ciertos equipos en la que alternativamente este proceso se realiza en Powershell del sistema operativo.

Como siguiente paso es fundamental aplicar la política en los entornos de Active Directory forzando la vía GPO, teniendo en cuenta que debe finalizar con la actualización del sistema operativo hacia un soporte de Windows Server 2008 o posteriores.

Análisis de resultados

Mediante este análisis del impacto en el presente servidor interno la falta de NLA en los servicios ejecutados y conocidos como RDP, esto logra demostrar que representa un cierto impacto entre los riesgos de los procesos administrativos y operativos donde generaliza la administración, mantenimiento y el control de acceso hacia sistemas financieros juntamente privilegiados a los factores técnicos.

Donde a medida que no se conlleve una configuración inmediata puede facilitar el acceso a usuarios no autorizados comprometiendo así la confidencialidad y continuidad operativa para ciertos servicios esenciales dentro de la empresa EMAPA.

3.2.3.14 Servidor 14 Desarrollo EMAPA

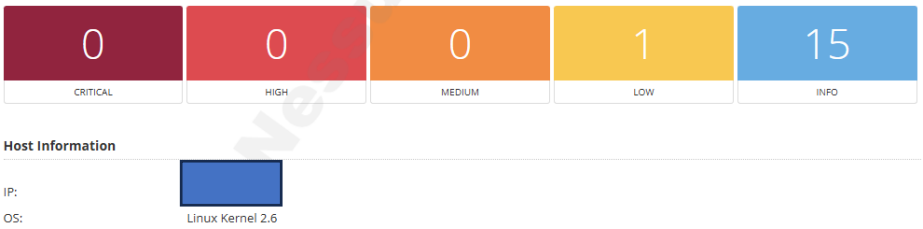


Figura 26. Resultado Servidor 14 Desarrollo EMAPA

- **10114 - ICMP Timestamp Request Remote Date Disclosure**

Identificación

Mediante la detección del servidor de desarrollo con el host remoto, prácticamente se considera como una marca del tiempo donde se refleja el protocolo ICMP, lo que permite que exista un ataque en obtener los datos de la fecha y la hora, en la que proporciona una información muy dependiente de la sincronización temporal. Este tipo de vulnerabilidades depende de la autenticación basada en el tiempo, donde refleja ataques más sofisticados, donde los sistemas de Linux se ejecuta una información con mayor precisión.

Remediación

Esta presente vulnerabilidad se puede mitigar mediante una gestión de la explotación en varios servicios de la red, juntamente con los protocolos ICMP en la que se diagnostica la red para que puedan ser explotados con a información no deseada en una mayor cantidad de ataques, en la que genera la limitación y puntos de red por la determinada posibilidad de explotar las vulnerabilidades como una divulgación que refuerza la postura de seguridad general del sistema principal, ejecutando las protección de las posibles acciones de ingresos no deseados dentro del servidor.

Análisis de resultados

Inicialmente se considera que a vulnerabilidad se enfoca con una vulnerabilidad baja, ya que la divulgación se identifica una hora exacta del servidor donde facilita una explotación desde otros sistemas que se enfoca en la autenticación con mayor relevancia en los protocolos de seguridad de la información que gestiona varios

procesos de mayor confianza, para ejecutar una filtración y la desactivación de las respectivas respuestas de las solicitudes para una mejora en la seguridad genera dentro de la infraestructura tecnológica de la empresa pública EMAPA.

3.2.3.15 Servidor 15 Cliente GIS EMAPA

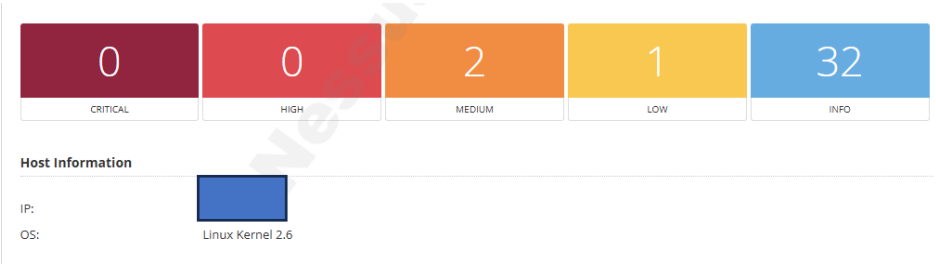


Figura 27. Resultado Servidor 15 Cliente GIS Emapa

- **51192 - SSL Certificate Cannot Be Trusted**

Identificación

Mediante el escaneo de seguridad del servidor se detecta una vulnerabilidad que tiene una relación entre el uso de un certificado digital no muy confiable, con la finalidad de no contener una emisión por el mismo servidor, en la que no contiene una alta confiabilidad, ni reconocimiento de forma pública, por otro lado, la firma del certificado no genera una verificación por usuarios expertos y ciertos usuarios no garantiza la conexión a servidor con la finalidad de validar la autenticación del mimo servicio implementado.

Evaluación del riesgo

En el caso de cada uno de los riesgos se fundamenta gracias a que el nivel d riesgo se conoce como medio, pero en base los archivos CVSS v3.0 se considera con un promedio de 6.5 y En el caso del archivo CVSS v2.0 con un promedio del 6.4 para llegar al énfasis que proyecta a una derivación de riesgos enfocados a la seguridad informática.

Impacto

Confidencialidad: No tiene una confidencialidad comprometida de forma parcial.

Integridad: No se establece a integridad de forma parcial

Disponibilidad: Esto no logra afectar mediante el impacto de los riesgos enfocado que genera la seguridad de la información.

Remediación

Ejecutar un remplazo del certificado auto firmado, que se considere con una confiabilidad alta en la que forme parte de la esencia de un modelo sincronizado a la clave pública de la infraestructura empresarial, con la finalidad que garantizan cierta autenticidad y validez de cierto servidor, donde conlleva con una mayor integridad dentro de las modificaciones de ciertos datos durante la transmisión, llevando a cabo la confidencialidad del cifrado y comunicación de la conectividad entre el cliente y servidor, para emitir una mejora de la base estructural que contiene los procesos de la determinada gestión en la identidad digitalizada de alta confiabilidad para todos los servicios que procesan estándares y normativas técnicas dentro la configuración virtualizada.

Análisis de resultados

Por medio del servidor identificado se vinculan dentro de los sistemas que gestiona la alta posibilidad del personal técnico y administrativo en la empresa EMAPA, con el objetivo de comprometer en una privacidad de los datos almacenados, debilidad de los mecanismos entre cliente y servidor. Finalmente, el aumento de los factores de riesgo bajo el complemento de interceptación y alteraciones del sistema.

- **57582 - SSL Self-Signed Certificate**

Identificación

Se encuentra utilizando un determinado certificado SSL con un autor firmado en la que pertenece, hacia un servicio que genera por el mismo emisor del certificado, donde genera una cadena de mayor confiabilidad para ser reconocida con su autenticidad, por otro lado , se tiene que los clientes no ejecutan una verificación mientras se encuentran conectados al servidor respectivo, donde posibilita la intercepción del atacante para la comunicación entre un cliente y servidor para llevar a cabo un análisis de la identidad del servidor. Donde esta vulnerabilidad anula ciertas garantías para ofrecer ciertos protocolos de dos tipos en la que consiste SSL y TLS.

Remediación

Implementar certificados de alta validez en la que fortalece una mayor confianza institucionales frente a una imagen de los usuarios, clientes en general y entidades de los sistemas de control que aborda los servicios de cada uno de los servidores internos dentro de la infraestructura tecnológica de la organización empresarial EMAPA, donde refleja una gobernanza para el usos adecuado de la contribución de las seguridad de diversas capas donde ciertas identidades no son verificadas por el servidor.

Análisis de resultados

En el caso del presente servidor se encuentra vinculado a un sistema, donde prioriza el gestionamiento de las información técnica en ciertos servicios básicos en la que conlleva un complemento de integridad hacia los datos gestionados en los servicios internos, donde reduce la confianza en los sistemas institucionales para la llevar a cabo la exposición de los riesgos legales y casos de puertos abiertos dentro de los servidores donde conlleva a tener una seguridad no beneficiada en la parte técnica.

3.2.3.16 Servidor 16 Help Desk

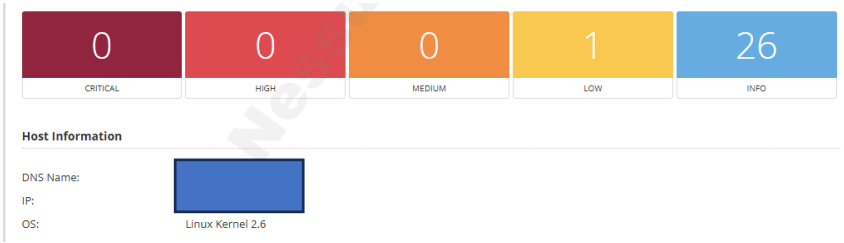


Figura 28. Resultado Servidor 6 Help Desk

- **10114 - ICMP Timestamp Request Remote Date Disclosure**

Identificación

La presente vulnerabilidad del servidor Help Desk se considera que se encuentra emulado en un sistema operativo, donde es de tipo ICMP como Timestamp Reques Remote Date Disclosure, en la permite conocer la fecha y la hora determinada del sistema correspondiente.

Remediación

Técnicamente esta vulnerabilidad genera una gran evidencia en la que consiste tener una debilidad en ciertos factores políticos de un control hacia ala exposición de los servicios auxiliares para el sistema operativo, donde refleja por medio de ciertos protocolos para las funciones dentro del ICMP, donde tiene la posibilidad de extraer metadatos del sistema, entonces para complementar esa solución implica en desactivar cualquier tipo de funcionalidad dentro del sistema ejecutado. En este caso, el servidor generalmente no necesita responder ciertas solicitudes del protocolo ICMP, para justificar de forma plena en el bloqueo.

Por otro lado, la remediación corresponde a un principio que se usa en los conjuntos con otro tipo de vulnerabilidades, en la que generaliza un gran impacto en su eliminación para contribuir la reducción del ataque de ciertos sistemas en la que refuerza una gran postura de seguridad general.

Análisis de resultados

En el caso de esta vulnerabilidad generalmente no compone de dato ni procesos críticos, pero si aborda cierta sincronización de los ataques de autenticaciones que se sincronizan en las horas específicas y adecuadas, pero se identifica ciertos sistemas que generaliza en base a la red enfocado a un mismo comportamiento, continuo para la preparación de asegurar que no se filtre ningún tipo de información, hacia las potencialidades de usuarios externos que intenten genera la conectividad cibernética en el servidor Help Desk.

3.2.3.17 Servidor 17 BD Servicios en Línea

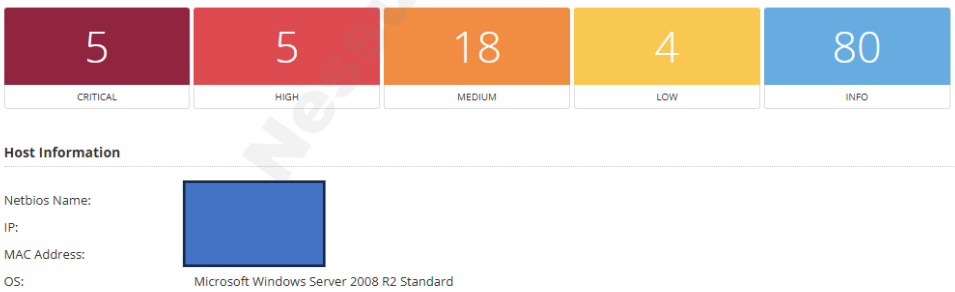


Figura 29. Resultado BD Servidor 17 Servicios en Línea

- **125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)**

Identificación

En este caso se ha identificado que contiene una vulnerabilidad crítica dentro del servidor interno, en la que tiene relación con el servicio del Escritorio Remoto RDP, donde logra demostrar que ciertas versiones antiguas del sistema de Windows, en la que concluye es conocida como BlueKeep, donde genera una ejecución con mayor integridad conexión remota sin necesidad de brindar la autenticación.

Evaluación del riesgo

Este riesgo el nivel se considera crítico, donde genera dos tipos de archivo tanto el CVSS v3.0 y CVSS v2.0, en la que se obtiene los siguientes resultados 9.8 y 10.00 para llegar a una probabilidad de alta explotación para el impacto e la seguridad de la información.

Impacto

Confidencialidad: Este proceso lleva a cabo a integridad un acceso no autorizado en los respectivos datos.

Integridad: Posee un riesgo de la modificación donde no requiere autorización-

Disponibilidad: Genera un riesgo de la denegación de ciertos servicios en la que tiene el objetivo de propagar de forma automática considerado de manera alta.

Remediación

Es importante aplicar los cambios necesarios de manera inmediata con la ayuda del soporte de la plataforma de Windows teniendo en cuenta que ciertos sistemas tanto como Windows XP, Server 2003, Microsoft se genera una publicación donde son excepcionales durante el mes de mayo del año 2019 para ejecutar una mitigación que falla de manera precisa.

Mitigación

Mediante este proceso es necesario deshabilitar los servicios RDP, donde demuestra que los sistemas vulnerables no es considerado indispensable, a su vez es indispensable

restringir un acceso hacia el puerto 3389 debido a que las redes no son confiables mediante las reglas administradas y configuradas por la herramienta del firewall, de tal manera que es necesario activar una autenticación dentro de la red, ya que tiene la posibilidad en añadir una determinada capa de proyección hacia los datos importantes de cada departamento que tiene la empresa, con el objetivo de implementar soluciones.

Análisis de resultados

En el caso de la explotación hacia el impacto de ciertos procesos críticos de la organización empresarial la vulnerabilidad puede permitir tomar el control total del servidor afectado, ya que puede contribuir por medio de operación en los servicios esenciales con ciertos accesos hacia las bases de datos, controles de los sistemas en la gestión interna y también un posible uso de plataformas de ataques hacia otros nodos externos como internos.

- **73756 - Microsoft SQL Server Unsupported Version Detection (remote check)**

Identificación

Durante el análisis de seguridad realizado al servidor expuesto en el puerto TCP 49497, se identificó la presencia de una instancia de Microsoft SQL Server en su versión 10.0.1600.0 correspondiente a SQL Server 2008. Según la información obtenida mediante análisis remoto, esta versión ha llegado al fin de su ciclo de vida (EOL) y ya no recibe actualizaciones de seguridad ni soporte por parte del fabricante. La instancia identificada fue SQLEXPRESS.

Evaluación de riesgos

Ejecutar una versión de SQL Server que ha quedado sin soporte oficial representa una amenaza crítica. La ausencia de parches de seguridad implica que cualquier vulnerabilidad descubierta posteriormente puede ser explotada sin posibilidad de mitigación por parte del proveedor. Además, estas versiones suelen tener múltiples vulnerabilidades documentadas públicamente, lo que facilita los ataques automatizados.

Impacto

Confidencialidad: Comprometida. Las vulnerabilidades no corregidas podrían permitir el acceso no autorizado a datos confidenciales almacenados en la base de datos.

Integridad: En riesgo. Un atacante podría alterar información sensible sin ser detectado, aprovechando debilidades conocidas del sistema.

Disponibilidad: Amenazada. Vulnerabilidades explotables pueden ocasionar caídas del servicio o denegaciones de acceso a los usuarios legítimos.

Remediación

La única solución efectiva consiste en realizar una actualización del motor de base de datos a una versión de SQL Server que actualmente esté en soporte oficial, como SQL Server 2019 o superior. Este proceso debe ir acompañado de una validación de compatibilidad de las aplicaciones dependientes y una migración segura de los datos. Es fundamental asegurarse de aplicar las últimas actualizaciones y parches de seguridad una vez completada la migración.

Mitigación

En caso de que la actualización inmediata no sea posible, se recomienda restringir el acceso al servicio SQL únicamente a las IP internas de confianza mediante listas de control de acceso (ACL) o configuración estricta en firewalld. También es aconsejable auditar constantemente los registros de acceso y monitorear la base de datos ante comportamientos anómalos que puedan indicar intentos de explotación.

Análisis de resultados

Este hallazgo demuestra una importante debilidad en la gestión del ciclo de vida de los sistemas críticos en el entorno de TI. Mantener en producción versiones obsoletas de software, especialmente sistemas de gestión de bases de datos como SQL Server, compromete gravemente la postura de seguridad de la organización. En el caso de EMAPA, es prioritario establecer una política clara de actualización tecnológica y cumplimiento de buenas prácticas, especialmente en infraestructuras que manejan datos sensibles y servicios esenciales.

- **20007 - SSL Version 2 and 3 Protocol Detection**

Identificación

Durante el escaneo del servicio expuesto en el puerto TCP 49497, correspondiente a una instancia de Microsoft SQL Server, se detectó que permite conexiones cifradas mediante los protocolos SSL 2.0 y SSL 3.0. Ambos protocolos son obsoletos y contienen múltiples vulnerabilidades criptográficas documentadas desde hace años. Esta configuración insegura permite que clientes utilicen cifrados débiles como DES-CBC3-SHA o incluso RC4-MD5, lo que representa un riesgo crítico para la confidencialidad e integridad de las comunicaciones.

Evaluación de riesgos

La activación de SSL 2.0 y 3.0 implica una exposición crítica, ya que un atacante podría llevar a cabo ataques de tipo man-in-the-middle, interceptar o manipular las sesiones, e incluso forzar una degradación del respectivo cifrado, como en el ataque conocido como POODLE. Dado que muchos clientes aún no implementan correctamente la negociación segura de protocolos, la posibilidad de explotación aumenta significativamente.

Impacto

Confidencialidad: Altamente comprometida. Un atacante con capacidades de red podría interceptar sesiones cifradas y desencriptar información sensible utilizando herramientas públicas conocidas.

Integridad: Existe la posibilidad de manipular el tráfico cifrado, aprovechando vulnerabilidades en los modos de cifrado como CBC.

Disponibilidad: Aunque no afecta directamente la disponibilidad del servicio, un ataque exitoso podría llevar a interrupciones o a la necesidad de deshabilitar el servicio para mitigar la brecha.

Remediación

Se debe acceder a la configuración del servidor SQL y deshabilitar de forma definitiva los protocolos SSL 2.0 y SSL 3.0. La solución recomendada es permitir únicamente conexiones a través de TLS 1.2 o superior, utilizando suites de cifrado modernas y

validadas por organismos como NIST. Esto puede implicar modificar el registro en sistemas Windows o ajustar parámetros de configuración en los archivos de OpenSSL si se utiliza una capa de cifrado externa.

Mitigación

En caso de no poder aplicar la remediación de inmediato, se recomienda limitar el acceso al puerto afectado mediante el firewall (firewalld) o una ACL a nivel de red que únicamente permita conexiones desde direcciones IP internas autorizadas. También se sugiere monitorear activamente los intentos de conexión con protocolos obsoletos y generar alertas ante eventos sospechosos.

Análisis de resultados

Este hallazgo evidencia la necesidad de realizar auditorías periódicas de seguridad sobre los protocolos de comunicación utilizados por los servicios críticos. A pesar de que SSL 3.0 ha sido oficialmente descontinuado desde hace varios años, su presencia en sistemas aún operativos indica una mala práctica de administración. Para instituciones como EMAPA, que manejan datos sensibles, mantener cifrados seguros no es una opción, sino una obligación que garantiza la confianza de los usuarios y el cumplimiento de estándares internacionales.

- **34460 - Unsupported Web Server Detection**

Identificación

Tiene el objetivo de detectar el servidor en la que ogra exponer ciertas vulnerabilidades mediante ciertas actualizaciones de seguridad donde es afectado por medio del puerto 80, donde refleja que la identificación que ejecuta Microsoft ISS 7.5 es prescindible para abordar un soporte EOS desde el 14 de enero del año 2020, en la que se define que ya no recibe ninguna actualización por lo que forma parte de Microsoft.

Evaluación de riesgo

Se considera alto debido a que tiene una exposición hacia lo múltiples CVEs donde no es corregido y a media de esta evaluación tiene un promedio de 10.0 y 7.5 en los dos archivos de suma importancia que se derivan y se analizan dentro de esta vulnerabilidad conocidos como: CVSS v3.0 y CVSS v2.0.

Impacto

Confidencialidad: Contribuye un acceso relativamente sensible hacia una confidencialidad alta.

Integridad: Genera una modificación de acceso riesgoso hacia el contenido con un factor de integridad alta.

Disponibilidad: Tiene la disponibilidad de generar una disponibilidad en los ataques DoS y otros factores que tiene el objetivo de considerases como alta.

Remediación

Es importante actualizar el servidor IIS hacia una versión soportada, donde se refleja ediciones de IIS 8.0, 8.5 y 10.0 del sistema operativo de Windows Server hasta a la versión disponible del año 2022, donde se da a conocer casos obsoletos con el objetivo de migrar hacia la versión más reciente.

Y para finalizar es recomendable eliminar un servicio específico donde no es necesario generar procesos críticos dentro de la organización empresarial.

Mitigación

Restringir el acceso al servidor por medio de las direcciones IPs confiables, donde se implementa un sistema Web aplican configuraciones reglamentarias de firewall, en la que sirve para detectar y bloquear ciertos patrones de ataque, por otro lado, es importante monitorear continuamente buscar los accesos correspondientes donde no es realmente autorizado en varios intentos de la explotación.

Y a media que conlleva este proceso garantiza revisar ciertos servicios donde dependen del servidor web.

Análisis de resultados

Es importante identificar que el servidor obsoleto se presenta una amenaza de manera directa, donde principalmente dispone de las seguridades en ciertos servicios en línea, donde generalmente brinda el acceso hacia portales de usuario, paneles de monitoreo e interfaces que refleja la mitigación en otros sistemas que integren APIs.

- **08797 - Unsupported Windows OS (remote)**

Identificación

Ejecutar dentro de un sistema operativo la exposición de EMAPA, donde las respectivas vulnerabilidades críticas por la falta de actualizaciones de seguridad el puerto afectado es de manera general, donde el servidor que se identifica es de Microsoft Windows Server 2008 R2, con el objetivo de alcanzar un soporte que no proporciona parches de seguridad.

Evaluación de riesgos

En este caso la evaluación de riesgo de la respectiva vulnerabilidad se considera crítico mediante la exposición de múltiples vulnerabilidades sin ninguna solución eficiente.

Impacto

Confidencialidad: El acceso no autorizado da a conocer hacia una información sensible de alto impacto.

Integridad: Corresponde de una integridad riesgosa en los datos de alta alteración en ciertos servicios.

Disponibilidad: Posee ciertos riesgos de las interrupciones juntamente con ransomware mediante el uso de ataques hacia nodos diferentes.

Remediación

Tiene el objetivo de actualizar un sistema operativo hacia versiones que aún son soportadas como Windows Server 2016, 2019 y 2022, donde es necesario verificar su compatibilidad con las aplicaciones y servicios antes de ejecutar la migración.

Por otro lado, es necesario reinstalar los servicios considerados como críticos en entornos más seguros alienados a los objetivos claros que posee la organización empresarial de EMAPA.

Mitigación

Si no se llega actualizar de forma inmediata realizar el proceso de aislar el servidor presente mediante la VLAN de red configurada para limitar ciertos accesos, aplicar las

políticas dentro de las condiciones de firewalld de forma estricta tomando en cuenta la desactivación como RDP, SMB v, IIS, etc.

Y para concluir con este ciclo de configuración es necesario realizar una documentación de auditoria continuamente con la ayuda de logs para visualizar el comportamiento de los sistemas que se ejecutan dentro de la empresa.

Análisis de resultados

El mantenimiento del sistema operativo es de mayor importancia para evitar amenazas directas hacia la infraestructura, donde llega afectar a servicios de operatividad institucional y cumplimiento regulatorio, siendo un punto desventajoso del servidor.

- **58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)**

Identificación

Esto es identificado por una vulnerabilidad alta mediante el servicio del escritorio remoto RDP, donde tiene en preferencia ejecutar un código para gestionar una incorrecta memoria del procesamiento por paquetes RDP, en la que un atacante es permitido por paquetes que son precisamente diseñados para ejecutar el código arbitrario de forma remota un impacto grave.

Evaluación de riesgo

Este género es precisamente para logra con una posibilidad de ejecución remota hacia el código de autenticación, gracias que ha que se determinada archivos CVSS v2.0 con un promedio del 9.3.

Impacto

Confidencialidad: Estos accesos tiene varios datos donde se represente a varios usuarios.

Integridad: Se logra ejecutar por medio de una conexión remota por medio de comandos sospechosos que se considera alta.

Disponibilidad: Posee en posibilidades donde la denegación de cada uno de los servicios puede ejecutar una infección por malware.

Remediación

Es necesario aplicar un parche de seguridad desde la parte de soporte desde Microsoft, donde corrige la vulnerabilidad, donde se considera como un factor alto para una versión más reciente de Windows.

Por otra parte, es necesario habilitar una autenticación a nivel de la red, con el objetivo de restringir el acceso RDP por varios usuarios autenticados y para finalizar este proceso es necesario configurar un nivel de seguridad de RDP a la medida SSL.

Mitigación

Por medio de los rasgos que le caracteriza este ciclo es fundamental deshabilitar RDP de manera temporal, donde netamente es centrado por las conexiones hacia el puerto 3389 permitiendo así ciertas direcciones IPs de alta confiabilidad, donde se monitorea varios logs en la que se identifica varios intentos de la conexión para analizar un determinado tráfico del servidor RDP.

Análisis de resultados

Tiene un compromiso donde netamente es permitido para abarcar un determinado control total de los servidores críticos, donde instala varios sitios de malware o herramientas de espionaje, con el objetivo de cifrar ciertos sistemas como afectaría disponibilidad, integridad y confidencialidad de los servicios digitales.

- **79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)**

Identificación

En los sistemas de EMAPA se ha identificado una vulnerabilidad crítica relacionada con el protocolo de seguridad Schannel, presente en versiones de Windows Server. Esta falla, reconocida como MS14-066, se manifiesta cuando el servidor procesa incorrectamente ciertos paquetes cifrados, lo que abre la posibilidad de que un atacante externo ejecute comandos maliciosos de manera remota. Esta amenaza afecta directamente a la seguridad de las conexiones que utilizan protocolos como TLS, incluyendo aquellas realizadas a través del puerto 3389, ampliamente usado para el Escritorio Remoto (RDP).

Evaluación de riesgos

El nivel de riesgo de esta vulnerabilidad es crítico, ya que permite la ejecución remota de código sin necesidad de interacción por parte del usuario o autenticación previa. Es decir, un atacante con conocimientos técnicos puede aprovechar esta falla para obtener control sobre el servidor. La criticidad también se debe a que el ataque puede realizarse desde cualquier red externa, incrementando el peligro para sistemas que estén expuestos a internet o conectados a redes poco seguras.

Impacto

Confidencialidad: La explotación de esta vulnerabilidad podría exponer información confidencial almacenada o transmitida en los servidores de EMAPA, incluyendo datos personales, credenciales de acceso o documentos institucionales.

Integridad: Un atacante podría manipular o alterar archivos del sistema o registros institucionales sin autorización, afectando la confianza en los datos.

Disponibilidad: Existe el riesgo de que se produzca una interrupción completa de los servicios, ya sea mediante un ataque de denegación de servicio o la instalación de programas que bloqueen el funcionamiento normal del servidor, como ransomware o software espía.

Remediación

Para corregir esta vulnerabilidad, se debe aplicar el parche oficial KB2992611, que ha sido desarrollado por Microsoft específicamente para solucionar este fallo en el componente Schannel. Esta actualización debe implementarse lo antes posible en todos los servidores que se encuentren dentro del alcance del riesgo. Adicionalmente, se recomienda activar la autenticación a nivel de red (NLA) en el servicio de RDP y establecer el nivel de seguridad en modo SSL/TLS, como una barrera adicional contra posibles ataques.

Mitigación

Mientras se aplica la solución definitiva, es importante restringir el acceso al puerto 3389 solo a direcciones IP específicas de confianza. También se puede deshabilitar temporalmente el acceso RDP si no es indispensable para la operación diaria. Estas

acciones deben ir acompañadas de una vigilancia continua del tráfico de red, análisis de registros del sistema y políticas de firewall más estrictas. Todo esto con el fin de detectar intentos de explotación tempranamente y limitar el impacto de un posible ataque.

Análisis de resultados

La presencia de esta vulnerabilidad en los servidores de EMAPA representa un riesgo elevado para la infraestructura tecnológica institucional. La posibilidad de que se ejecute código malicioso de forma remota pone en juego no solo los sistemas operativos, sino también los servicios que dependen de ellos. Si no se toman medidas correctivas y preventivas, los atacantes podrían tomar control total del entorno, comprometiendo seriamente la disponibilidad, integridad y confidencialidad de los sistemas críticos. Es indispensable actuar con urgencia para cerrar esta brecha de seguridad y proteger el entorno digital de la organización.

- **97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)**

Identificación

Dentro de los servidores internos de EMAPA, se ha detectado una vulnerabilidad crítica relacionada con el servicio SMBv1, específicamente identificada como MS17-010, conocida popularmente por explotar ciertos conflictos. Esta falla permite a un atacante ejecutar código malicioso de forma remota a través del puerto 445, mediante paquetes diseñados para manipular de forma indebida el protocolo SMB. Este tipo de vulnerabilidad ha sido aprovechada en ataques globales como WannaCry y Petya, afectando gravemente infraestructuras públicas y privadas. El sistema operativo más afectado en este contexto es Windows Server 2008 R2, aún presente en algunos entornos de EMAPA.

Evaluación de riesgos

El nivel de riesgo de esta vulnerabilidad es crítico, ya que no requiere autenticación y puede ser explotada de manera remota. Una vez comprometido el servidor, el atacante podría distribuir malware o ransomware sin intervención del usuario. El riesgo

aumenta al mantener habilitado el protocolo SMBv1, que actualmente es obsoleto y carente de medidas modernas de protección, haciendo que el entorno sea altamente vulnerable a amenazas persistentes y automáticas, como lo demostró el ataque WannaCry en 2017.

Impacto

Confidencialidad: La vulnerabilidad permite la exposición de archivos y datos institucionales que pueden ser descargados sin autorización, comprometiendo la privacidad de la información sensible.

Integridad: Existe la posibilidad de modificación, alteración o corrupción de datos críticos almacenados en los servidores, lo que podría afectar la veracidad de la información institucional.

Disponibilidad: El impacto puede derivar en la inoperatividad total del sistema, ya que muchos de los ataques asociados con esta vulnerabilidad bloquean el acceso mediante cifrado de archivos (ransomware), impidiendo el funcionamiento normal de los servicios que dependen del servidor.

Remediación

La solución principal es aplicar de forma urgente las actualizaciones de seguridad publicadas por Microsoft, específicamente el parche KB4013389 correspondiente a la actualización MS17-010. Además, es necesario deshabilitar permanentemente el protocolo SMBv1, dado que su uso representa un riesgo innecesario. Esta acción debe ir acompañada de una revisión del resto de servicios dependientes del protocolo SMB, migrando en su lugar al uso de SMBv2 o SMBv3, que sí ofrecen soporte activo y mecanismos de seguridad modernos.

Mitigación

Es necesario aplicar las actualizaciones de forma inmediata, se debe implementar una segmentación de red que limite el acceso al puerto 445 únicamente a dispositivos internos autorizados. También es recomendable bloquear el tráfico SMB entrante y saliente a través de reglas en el firewall, y monitorear de manera constante los logs de acceso en busca de comportamientos anómalos. Otra acción temporal de mitigación es

el uso de VLANs específicas para aislar los servidores antiguos o vulnerables, minimizando así la exposición general.

Análisis de resultados

La existencia de esta vulnerabilidad en los sistemas de EMAPA representa una amenaza directa a la seguridad operativa de los servidores institucionales. La falta de aplicación de parches y la permanencia de servicios obsoletos como SMBv1 abren la puerta a ciberataques de gran impacto, los cuales pueden paralizar actividades esenciales. Este tipo de fallas deja en evidencia la necesidad urgente de adoptar una política de actualización continua, gestión de vulnerabilidades y modernización tecnológica que permita preservar la estabilidad, la seguridad y el cumplimiento normativo de la institución.

- **57690 - Terminal Services Encryption Level is Medium or Low**

Identificación

Se identificó que el servicio de Escritorio Remoto (Terminal Services) del servidor en análisis mantiene un nivel de cifrado medio. Esta configuración implica que las sesiones establecidas por el puerto TCP 3389 están utilizando mecanismos criptográficos débiles, lo cual representa un riesgo frente a intentos de interceptación de datos. El nivel actual de cifrado detectado corresponde a “Medium”, lo cual no es adecuado para entornos que manejan información sensible o de carácter institucional, como es el caso de EMAPA.

Remediación

La acción principal para mitigar este riesgo consiste en elevar el nivel de cifrado de las sesiones RDP en el servidor. Se recomienda configurar el nivel de cifrado en modo High o, de preferencia, FIPS Compliant, garantizando el uso de algoritmos más seguros avalados por estándares internacionales. Este cambio debe realizarse desde las directivas locales del servidor o mediante políticas de grupo (GPO), y es importante verificar que todos los clientes remotos sean compatibles con estos niveles de cifrado.

Análisis de resultados

El mantenimiento de buenas prácticas de cifrado en los servicios críticos como RDP es clave para reducir vectores de ataque. En el caso de EMAPA, garantizar comunicaciones remotas seguras evita vulnerabilidades de espionaje o robo de información institucional. Este hallazgo resalta la importancia de revisar configuraciones por defecto que en muchos casos pasan desapercibidas, pero que comprometen de forma silenciosa la seguridad de toda la infraestructura.

3.2.3.18 Servidor 18 Financiero Antiguo

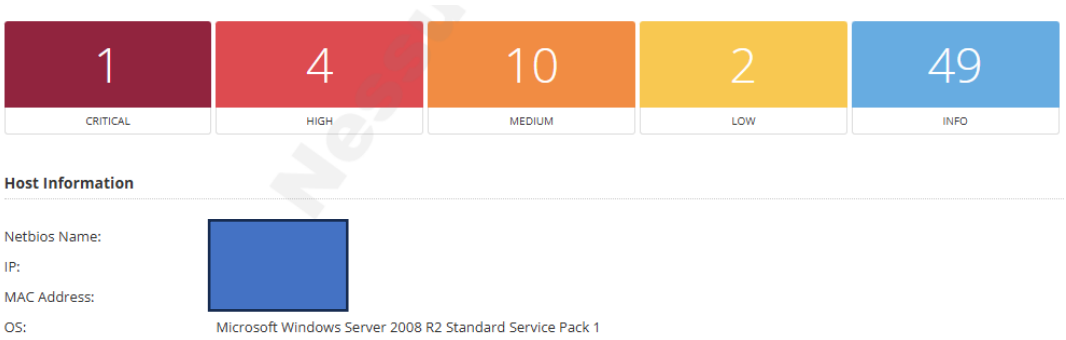


Figura 30. Resultado Servidor 18 Financiero Antiguo

- **108797 - Unsupported Windows OS (remote)**

Identificación

Mediante el entorno de red, se detectó que uno de los servidores ejecuta el sistema operativo Microsoft Windows Server 2008 R2 Standard con Service Pack 1. Esta versión ha sido oficialmente descontinuada por Microsoft y ya no recibe actualizaciones de seguridad ni soporte técnico desde enero de 2020.

Evaluación de riesgos

El hecho de que un sistema operativo esté fuera del ciclo de vida de soporte representa un riesgo crítico. Cualquier vulnerabilidad presente en esta versión ya no será parcheada por el fabricante, y al estar ampliamente documentadas en la comunidad de ciberseguridad, son susceptibles a ser explotadas por atacantes sin dificultad.

Impacto

Confidencialidad: En peligro. La información almacenada o transmitida por este servidor puede ser interceptada o accedida sin autorización mediante exploits conocidos.

Integridad: Vulnerable. Existe la posibilidad de que un atacante modifique archivos o configuraciones del sistema sin ser detectado.

Disponibilidad: En riesgo. Un atacante puede aprovechar vulnerabilidades del sistema para provocar fallos del servidor o interrupciones en los servicios ofrecidos.

Remediación

La acción más adecuada y efectiva es llevar a cabo una migración a una versión de Windows Server actualmente soportada, como Windows Server 2019 o 2022. Esta migración debe ser planificada cuidadosamente, asegurando que las aplicaciones y servicios en ejecución sean compatibles con el nuevo sistema operativo y que se realice un respaldo completo antes de la actualización.

Mitigación

Por ciertas razones es necesario implementar ciertas medias donde brinda una restricción hacia el acceso de este servidor por medo de ciertos segmentos de la red interna que forma parte de la empresa EMAPA, a medida que refleja este ciclo se logra implementar ciertas reglas relativamente estrictas juntamente con el firewall del sistema y el parámetro de la red, con ciertos monitoreos en tiempo real.

Análisis de resultados

La respectiva gestión de infraestructura tecnológica tiene el objetivo de operar con sistemas sin soporte es una práctica que expone a la organización a riesgos innecesarios, especialmente en contextos donde se maneja información crítica o se ofrecen servicios esenciales. En el caso de EMAPA, es indispensable implementar un plan de renovación tecnológica que contemple el reemplazo de sistemas obsoletos por plataformas actualizadas y seguras, alineadas con las buenas prácticas del sector.

- **58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)**

Identificación

Durante el escaneo de seguridad realizado a la infraestructura de EMAPA, se detectó una vulnerabilidad crítica relacionada con el protocolo RDP (Remote Desktop Protocol), identificada por el plugin 58435. Esta vulnerabilidad está descrita en el boletín de seguridad MS12-020 de Microsoft y afecta a diversas versiones del sistema operativo Windows. El hallazgo se presentó específicamente en el puerto TCP 3389, el cual es utilizado por el servicio de escritorio remoto.

Evaluación de riesgo

La vulnerabilidad permite la ejecución remota de código sin necesidad de autenticación previa. Esto quiere decir que un atacante, aprovechando esta falla, puede ejecutar comandos arbitrarios en el sistema comprometido, con los mismos privilegios del servicio afectado. La causa se debe a un error en la forma en que el protocolo RDP gestiona ciertos objetos en memoria que han sido incorrectamente inicializados o ya han sido eliminados.

Además, este mismo fallo puede explotarse para provocar una denegación de servicio (DoS), causando que el sistema se bloquee o reinicie inesperadamente.

Impacto

Confidencialidad: Puede verse gravemente comprometida si un atacante accede al sistema y extrae información sensible.

Integridad: Está en riesgo ya que el atacante podría modificar archivos, configuraciones o instalar software malicioso.

Disponibilidad: Vulnerable a interrupciones. Un exploit puede hacer que el sistema deje de prestar servicios a usuarios legítimos.

Remediación

La solución oficial es aplicar los parches de seguridad liberados por Microsoft para cada versión de Windows afectada. Estos parches están disponibles para sistemas como Windows XP, Windows Vista, Windows 7, Windows Server 2003, 2008 y 2008

R2. En caso de que se utilicen sistemas obsoletos como Windows 2000, se requiere un contrato de soporte extendido con Microsoft para poder acceder a las actualizaciones correspondientes.

Análisis de resultados

Tiene el objetivo de analizar una debilidad crítica en la superficie de ataque expuesta por EMAPA al utilizar versiones de Windows que no cuentan con configuraciones seguras por defecto. La explotación de esta vulnerabilidad es pública y se encuentra disponible en múltiples frameworks de ataque como Metasploit, Core Impact y CANVAS, lo cual incrementa significativamente el nivel de amenaza. Es urgente implementar las actualizaciones de seguridad y considerar el endurecimiento general de los servicios expuestos a la red para prevenir accesos no autorizados.

- **79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)**

Identificación

En el proceso de evaluación de seguridad en los servidores de EMAPA, se identificó una vulnerabilidad crítica asociada al canal seguro de comunicación de Windows, conocida como MS14-066 y catalogada con el plugin 79638. Esta vulnerabilidad se presenta en el componente Schannel (Secure Channel), encargado de gestionar el tráfico cifrado mediante protocolos como TLS y SSL. El hallazgo se detectó en el puerto TCP 3389, comúnmente utilizado por el servicio de Escritorio Remoto (RDP).

Evaluación de riesgos

La ejecución remota de código (RCE), lo cual representa una amenaza seria para la infraestructura de red. El error ocurre debido al mal manejo de ciertos paquetes malformados por parte de Schannel. Si un atacante logra enviar paquetes especialmente diseñados hacia un servidor Windows vulnerable, podría ejecutar código arbitrario con los mismos privilegios del proceso afectado.

Impacto

Confidencialidad: Altamente comprometida, ya que un atacante podría interceptar o exfiltrar información sensible desde el servidor afectado.

Integridad: En riesgo, puesto que el atacante puede modificar archivos o instalar malware que altere el funcionamiento del sistema.

Disponibilidad: Peligra, ya que la explotación de esta falla puede causar fallos en el servicio o bloqueos en el sistema.

Remediación

En el caos de Microsoft logro publicar las actualizaciones de seguridad para corregir esta vulnerabilidad en sistemas operativos como Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows Server 2008, 2008 R2, 2012 y 2012 R2. La solución inmediata es aplicar el parche correspondiente con el identificador KB2992611, disponible a través de Windows Update o el sitio oficial de Microsoft.

Mitigación

En este proceso es necesario aplicarlas siguientes medidas para reducir una cierta restricción mediante el acceso del puerto 3389, donde es interpretado por las reglas del firewall, en la que permite y brinda conexiones desde las respectivas redes internas con mayor autorización, donde asegura versiones actualizadas y seguras juntamente con los protocolos TLS.

Análisis de resultados

Esta vulnerabilidad ha sido ampliamente documentada y es explotable a través de herramientas como Core Impact, lo que demuestra que su explotación es técnica y operativamente viable. Su presencia en los servidores de EMAPA representa un riesgo crítico, ya que podría permitir a un atacante remoto comprometer completamente el sistema sin interacción del usuario ni credenciales. Por otra parte, es necesario aplicar los parches indicados y reforzar las políticas de seguridad en los canales de comunicación cifrados para proteger los activos tecnológicos de la institución.

- **97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)**

Identificación

En el caso de la seguridad los servidores internos de EMAPA, se detectó una vulnerabilidad crítica en el servicio de compartición de archivos de Microsoft conocido como SMBv1. La detección se dio mediante el plugin 97833, el cual hace referencia a múltiples fallas de seguridad identificadas en el boletín MS17-010, más conocido por su vinculación con exploits ampliamente utilizados como ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY. El puerto implicado en este hallazgo es el 445/TCP, que corresponde al protocolo CIFS (Common Internet File System) utilizado por SMB.

Evaluación de riesgos

Esta vulnerabilidad se clasifica como crítica, ya que permite a un atacante ejecutar código malicioso de forma remota sin necesidad de autenticarse previamente. El fallo se produce debido a una mala gestión de ciertos paquetes enviados al servidor SMB, lo que permite la ejecución de comandos arbitrarios en el sistema afectado. Exploits como ETERNALBLUE fueron utilizados en ataques globales de ransomware como WannaCry, Petya y EternalRocks, demostrando el alcance real de este tipo de debilidades en entornos no parcheados.

Impacto

Confidencialidad: Severamente afectada, ya que los atacantes pueden acceder a archivos internos sin autorización.

Integridad: En riesgo crítico, dado que se pueden modificar o sobrescribir archivos del sistema o datos corporativos.

Disponibilidad: Potencialmente comprometida, ya que la explotación puede ocasionar bloqueos del sistema o despliegues de ransomware que inutilicen los servicios.

Remediación

Mediante las actualizaciones de seguridad específicas para corregir esta falla en versiones como Windows Vista, 7, 8.1, 10, Server 2008, 2012, 2016, así como en sistemas obsoletos como Windows XP y Server 2003, dada la magnitud del problema. La solución principal es aplicar de forma inmediata el boletín de seguridad MS17-010, contenido en el parche KB4013389.

Mitigación

Es necesario generar un deshabilitación donde proporciona ciertas instrucciones por parte de versiones y actualizaciones de Microsoft, donde es necesario bloquear el puerto 445 nivel del firewall perimetral para impedir ciertas conexiones de manera externa, que no autoriza, mediante la restricción del uso SMB en la red interna con la finalidad de implementar un monitoreo de mayor continuidad para detectar varios intentos de explotación en la conexión de forma remota.

Análisis de resultados

Esta vulnerabilidad es una de las más explotadas a nivel mundial, con múltiples herramientas de ataque disponibles públicamente como Metasploit, CANVAS y Core Impact. Su presencia en los servidores de EMAPA representa un riesgo inminente que debe ser tratado con máxima prioridad. La explotación de MS17-010 no requiere interacción del usuario, por lo que cualquier exposición al puerto 445 puede derivar en una intrusión masiva, cifrado de datos o propagación lateral del ataque a otros equipos internos. Se recomienda, además de aplicar los parches y mitigar el acceso externo, realizar un análisis forense para verificar si ha existido algún intento de explotación previa.

- **90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)**

Identificación

Mediante el proceso de evaluación de seguridad realizado sobre los servidores internos de EMAPA, se detectó una vulnerabilidad relacionada con los protocolos de autenticación de Windows, específicamente en SAM (Security Account Manager) y LSAD (Local Security Authority - Domain Policy). Esta falla de seguridad fue

identificada por el plugin 90510 y está documentada en el boletín de seguridad MS16-047, también conocida bajo el nombre de Badlock. El vector afectado corresponde a conexiones DCE/RPC a través del puerto dinámico 49171/TCP, utilizado comúnmente por servicios de administración remota de Windows.

Remediación

Lo solución correspondiente a esta vulnerabilidad está incluido en el boletín de seguridad MS16-047, específicamente bajo el identificador KB3148527. Se recomienda verificar la instalación de este parche en todos los equipos expuestos, especialmente aquellos que funcionen como controladores de dominio o almacenes de autenticación.

Análisis de resultados

La presencia de esta vulnerabilidad en los sistemas de EMAPA indica un riesgo medio, pero que no debe subestimarse debido a su potencial de ser utilizado como puerta de entrada para ataques más avanzados. Aunque su explotación requiere condiciones específicas para un escenario comprometido como una red con usuarios con equipos vulnerables o redes inalámbricas mal protegidas podría facilitar el acceso no autorizado a servicios críticos. Además, esta vulnerabilidad fue ampliamente publicitada en su momento bajo el nombre Badlock, lo que motivó la creación de exploits específicos, aumentando el riesgo de ser utilizada por atacantes automatizados.

3.2.3.19 Servidor 19 Comercial

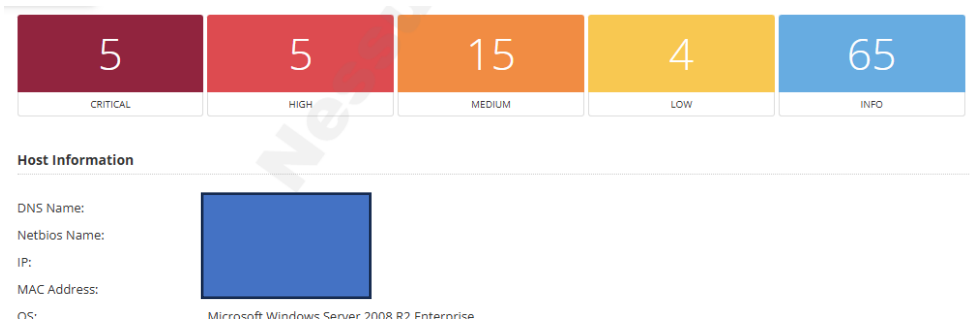


Figura 31. Resultado Servidor 19 Comercial

- **125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)**

Identificación

Durante el análisis de seguridad efectuado en los servidores internos de EMAPA, se detectó una vulnerabilidad crítica relacionada con el protocolo de Escritorio Remoto (RDP) de Microsoft. Esta debilidad fue identificada mediante el plugin 125313 de Nessus, el cual alerta sobre la presencia de la vulnerabilidad CVE-2019-0708, comúnmente conocida como BlueKeep. El puerto afectado es el 3389/TCP, correspondiente al servicio de RDP.

Evaluación de riesgos

Esta vulnerabilidad permite que un atacante remoto, sin autenticación previa, pueda ejecutar código arbitrario en el sistema vulnerable. El fallo se encuentra en el manejo incorrecto de solicitudes RDP especialmente diseñadas, lo que habilita la ejecución remota de código con privilegios elevados. Debido a su naturaleza, este tipo de fallo puede propagarse automáticamente entre sistemas, similar a un gusano, lo que multiplica el impacto en redes internas mal segmentadas o desactualizadas.

La amenaza es especialmente crítica en entornos corporativos donde el servicio de escritorio remoto es utilizado para administración remota, ya que un ataque exitoso podría derivar en control total del sistema, instalación de malware, cifrado de archivos (ransomware), o propagación lateral hacia otros servidores.

Impacto

Confidencialidad: Completamente comprometida; el atacante puede acceder a toda la información contenida en el sistema afectado.

Integridad: Totalmente vulnerable; el atacante puede modificar, borrar o introducir datos maliciosos.

Disponibilidad: Severamente afectada; el atacante puede dejar el sistema fuera de servicio o utilizarlo para ejecutar ataques sobre otros equipos.

Remediación

En este caso Microsoft forma parte de un conjunto de son dirigidos los sistemas operativos más afectados, en la que incluye Windows XP, Windows Server 2003, Windows 7, Windows Server 2008 y Windows Server 2008 R2.

Donde la solución de remediación sería en aplicar ciertos boletines de ciertas seguridades donde emite Microsoft, donde genera una corrección a esta vulnerabilidad crítica.

Mitigación

Es necesario ejecutar las siguientes acciones de mitigación, donde se deshabilita un servicio RDP en la que se considera que no es indispensable, tambien es importante restringir el acceso al puerto detectado, donde es necesario habilitar la autenticación a un nivel de la red NLA, en la que prioriza ciertos sistemas vulnerables para aplicar una microsegmentación al momento de limitar la configuración de la red por ciertas propagaciones de las amenazas.

Análisis de resultados

Representa una de las amenazas más peligrosas a nivel de infraestructura, debido a su capacidad de ejecución remota sin autenticación y su potencial para replicarse dentro de redes mal protegidas. Por otro lado, a remediación de esta vulnerabilidad debe tratarse como una prioridad crítica dentro del plan de mejora de la postura de ciberseguridad de EMAPA. La aplicación de parches y controles compensatorios no solo es esencial, sino urgente para evitar incidentes mayores.

- **73756 - Microsoft SQL Server Unsupported Version Detection (remote check)**

Identificación

Por medio de este proceso de evaluación de seguridad realizado en los servidores internos de EMAPA, se identificó una vulnerabilidad crítica relacionada con el motor de base de datos Microsoft SQL Server. Esta debilidad fue detectada a través del plugin 73756 de Nessus, el cual informa sobre la presencia de una versión obsoleta e insegura del motor de base de datos, específicamente la versión 9.0.3042.0, correspondiente a

Microsoft SQL Server 2005. El servicio afectado está expuesto en el puerto 1433/TCP, utilizado para conexiones remotas al servidor SQL.

Evaluación de riesgos

La principal amenaza radica en el hecho de que esta versión de SQL Server ha alcanzado su fin de vida útil (EOL), lo cual implica que Microsoft ya no proporciona parches de seguridad, actualizaciones funcionales ni soporte técnico. Como resultado, cualquier vulnerabilidad descubierta en esta versión queda permanentemente sin solución por parte del fabricante, dejando al sistema en un estado de riesgo constante y creciente.

Además, el uso de versiones obsoletas en servicios expuestos como SQL Server abre una puerta crítica a posibles ejecuciones remotas de código, escalamientos de privilegios, accesos no autorizados o filtraciones de datos. Estas condiciones convierten al sistema en un objetivo atractivo para atacantes, especialmente si se encuentra conectado a redes internas con otros activos sensibles.

Impacto

Confidencialidad: Altamente comprometida. Un atacante podría obtener acceso total a las bases de datos alojadas, incluyendo credenciales, registros financieros, información de usuarios, entre otros.

Integridad: Vulnerable. Es posible alterar, eliminar o insertar datos maliciosos dentro de la base de datos sin ser detectado.

Disponibilidad: En riesgo. El sistema puede ser deshabilitado, corrompido o utilizado como punto de entrada para ataques más amplios en la infraestructura interna.

Remediación

La manera más efectiva de mitigar esta vulnerabilidad es actualizando Microsoft SQL Server a una versión compatible. Las versiones actuales, como SQL Server 2019 y SQL Server 2022, no solo abordan vulnerabilidades identificadas previamente, sino que también incluyen mejoras en el rendimiento, mejor soporte para la encriptación y mecanismos de seguridad avanzados.

Aparte de la actualización, se deben realizar copias de seguridad completas de las bases de datos, validar la compatibilidad de las aplicaciones existentes, migrar con pruebas e implementar cambios en producción.

Mitigación

Precisamente esto sugiere en planificar la limitación de un acceso dentro del puerto 1433, donde específicamente se implementa una segmentación, donde se monitorea ciertos accesos para aplicar ciertos cifrados, en la que no se encuentran habilitados por medio de un ataque al servidor SQL.

Análisis de resultados

Usar una versión obsoleta de Microsoft SQL Server se considera una violación grave en la estrategia de mantenimiento, actualización y mejora del software. En entornos comerciales como el de EMAPA, que implica manejar información crítica y sensible, la existencia de tales vulnerabilidades representa un riesgo significativo, o incluso la probabilidad de una violación de datos, pérdida de integridad y interrupciones en el servicio.

Debido a la puntuación de CVSS v3.0 de 10.0 para la vulnerabilidad identificada, que es la puntuación más alta posible, y teniendo en cuenta que la vulnerabilidad trata sobre un servicio tan fundamental y crítico como una base de datos nos lleva a concluir que la remediación debe tratarse como un asunto absolutamente urgente dentro del plan de iniciativa de mejora de ciberseguridad institucional.

No actualizar este servicio representa un riesgo para la continuidad operativa del sistema, la reputación organizacional e incluso la responsabilidad organizacional bajo marcos de incidentes, seguridad y legales.

- **58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)**

Identificación

Mientras se llevaba a cabo la evaluación de seguridad sobre la infraestructura interna de EMAPA, hubo un riesgo crítico relacionado con el protocolo de escritorio remoto (RDP) en sistemas operativos Windows. Esta vulnerabilidad fue descubierta utilizando

el plugin 58435 de Nessus, que corresponde al boletín de seguridad MS12-020 publicado por Microsoft. El servicio en cuestión se ejecuta en el puerto 3389/TCP, que generalmente se asocia con terminales de escritorio remoto (Servicios de Terminal).

La debilidad proviene de una implementación inadecuada del manejo de objetos dentro del espacio de memoria desasignado durante la manipulación de la sesión RDP. En particular, el error ocurre cuando un sistema accede a objetos mal inicializados o ya eliminados, lo que permite a un atacante ejecutar código arbitrario en el sistema afectado.

Evaluación de riesgos

Esta debilidad representa un riesgo alto para la seguridad de los sistemas de EMAPA, ya que un atacante remoto, sin necesidad de autenticación previa, podría explotar el error mediante el envío de paquetes RDP maliciosamente diseñados. En condiciones vulnerables, esto permitiría la ejecución remota de código con privilegios del sistema, lo cual podría derivar en el control total del equipo afectado.

Adicionalmente, esta vulnerabilidad ha sido integrada en herramientas de explotación como Metasploit, CANVAS y Core Impact, lo que facilita su utilización incluso por atacantes con conocimientos técnicos limitados. La amenaza también incluye la posibilidad de denegación de servicio (DoS) si el sistema colapsa como consecuencia de la explotación.

Impacto

Confidencialidad: Gravemente comprometida. El atacante puede acceder sin restricciones a la información almacenada en el sistema.

Integridad: Totalmente en riesgo. Puede modificarse o eliminarse información, y ejecutarse código arbitrario sin detección.

Disponibilidad: Afectada severamente. El sistema puede quedar inoperativo o ser utilizado como plataforma para lanzar ataques contra otros equipos.

Remediación

Forma parte de una solución donde en aplicar ciertas condiciones de parches en la que son disponibles en ciertos sistemas operativos, donde se destacan los sistemas

operativos de Windows 2000, por lo cual requiere un servicio RDP, que generalmente acepte ciertas conexiones desde varios equipos de la autenticación a un nivel de red que mitiga una cierta exposición del fallo.

Mitigación

Es necesario deshabilitar de forma temporal RDP, donde es necesario restringir un acceso hacia el puerto RDP con la finalidad de generar ciertas habilitaciones de autenticaciones para actualizar un respectivo monitoreo que son asociados a esta vulnerabilidad para segmentar la red de manera óptima de los servidores internos de forma crítica.

Análisis de resultados

Esto constituye una amenaza significativa para la infraestructura de EMAPA, debido a que permite la ejecución remota de código sin autenticación, lo que la convierte en un vector común de ataques automatizados y ransomware.

El uso de RDP sin las configuraciones adecuadas y en versiones de Windows sin actualizaciones expone a la organización a incidentes graves que podrían comprometer información sensible, afectar la operación de los sistemas y dañar la reputación institucional.

Debido a su alto puntaje CVSS (9.3) y la existencia pública de herramientas para su explotación, se concluye que su corrección debe tratarse como una prioridad de seguridad inmediata. La aplicación oportuna de los parches, junto con controles compensatorios, es fundamental para reducir el riesgo y fortalecer la postura de ciberseguridad de EMAPA frente a ataques remotos.

- **18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness**

Identificación

Mediante el proceso de evaluación de seguridad en los servidores internos de EMAPA, se ha detectado una debilidad asociada al servicio de Escritorio Remoto (RDP) que escucha en el puerto TCP/3389. La detección corresponde al plugin 18405 de Nessus, el cual evidencia una vulnerabilidad susceptible a ataques de tipo hombre en el medio (Man-in-the-Middle, MiTM).

Este fallo se origina debido a que la versión afectada del servicio RDP no valida adecuadamente la identidad del servidor durante el establecimiento de sesiones cifradas. En otras palabras, el cliente RDP no verifica el certificado del servidor al iniciar la comunicación, permitiendo que un atacante pueda interceptar y manipular la conexión sin ser detectado.

Remediación

Es necesario forzar el uso de las SSL, donde varios entornos de Microsoft, permite ejecutar ciertas ejecuciones de escritorio remoto, donde verifican los certificados con ciertos servicios en RDP en la que generaliza una validez de entidades altamente confiables, para aplicar segmentaciones con ciertas restricciones en el acceso al servicio RDP.

Análisis de resultados

En la presente vulnerabilidad se genera una implementación débil del cifrado en versiones antiguas del protocolo RDP. El uso de una clave RSA incrustada públicamente conocida representa un fallo crítico en la seguridad del canal de comunicación, especialmente en entornos donde no se cuenta con mecanismos de autenticación mutua entre cliente y servidor.

Aunque su puntuación CVSS es moderada (6.5 en la versión 3.0), el contexto operativo y las características de la red determinan el nivel real de exposición. En el caso de EMAPA, donde se manejan datos sensibles de carácter institucional, se recomienda desplegar medidas correctivas de forma prioritaria para evitar filtraciones de credenciales o accesos indebidos.

Este hallazgo refuerza la necesidad de revisar todas las configuraciones relacionadas con servicios de acceso remoto, garantizando que se apliquen estándares modernos de cifrado y autenticación, protegiendo así los activos informáticos de la organización frente a amenazas internas y externas.

3.2.3.20 Servidor 20 Documental

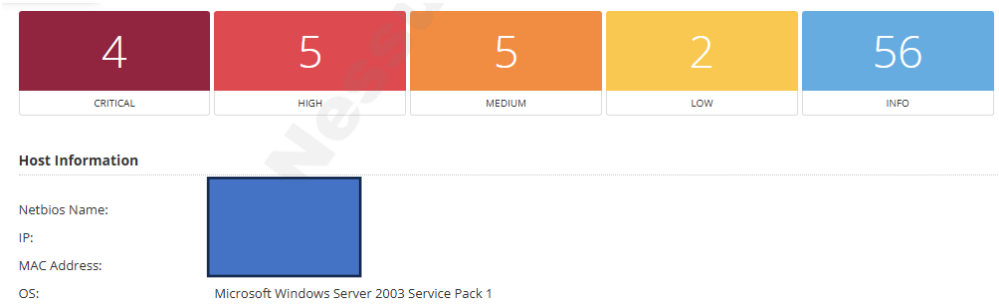


Figura 32. Resultado Servidor 20 Documental

- **97995 - IBM Domino SEoL (<= 1.3.x)**

Identificación

Durante el proceso de análisis de vulnerabilidades realizado en los servidores internos de EMAPA, se detectó que uno de los sistemas cuenta con una versión obsoleta del software IBM Domino, anteriormente conocido como IBM Lotus Domino. Según el escaneo realizado, la versión instalada corresponde a la 5.0.11, que dejó de recibir soporte por parte del fabricante el 30 de septiembre de 2005. Esta información fue proporcionada por el plugin 97995 de Nessus, el cual identificó el servicio ejecutándose en el puerto 25/TCP (SMTP).

Evaluación de riesgos

El uso de software que ha alcanzado su ciclo de vida (End of Life - EOL) representa una amenaza crítica para la seguridad de los sistemas de información. En este caso, IBM Domino en su versión 5.0.11 no recibe actualizaciones de seguridad desde hace más de 19 años, lo cual implica que cualquier vulnerabilidad descubierta desde entonces permanece sin solución. Esto convierte al sistema en un objetivo fácil para atacantes que buscan explotar fallas conocidas, incluso mediante herramientas automatizadas.

Impacto

Confidencialidad: Altamente comprometida debido a la posibilidad de acceso no autorizado a la información almacenada o transmitida por el servidor Domino.

Integridad: En riesgo, ya que el atacante podría manipular datos del sistema sin restricciones.

Disponibilidad: Severamente comprometida, al ser posible la explotación de vulnerabilidades para provocar fallos en el servicio o realizar ataques de denegación de servicio (DoS).

Remediación

La solución recomendada es realizar una actualización inmediata del software IBM Domino a una versión actualmente soportada por IBM. Las versiones más recientes han recibido parches de seguridad y mejoras que mitigan vulnerabilidades conocidas. Además, es recomendable realizar una revisión integral de configuración y aplicar buenas prácticas de seguridad en el nuevo entorno.

Mitigación

Logra restringir un acceso al puerto 25 donde permite ejecutar conexiones desde ciertas conexiones IPs confiables, en la que genera un monitoreo del tráfico aplicando el protocolo SMTP y, por otra parte, es importante asilar el servidor mediante un entorno de producción para evaluar las posibilidades hacia el servicio temporal.

Análisis de resultados

La presencia de esta vulnerabilidad refleja una brecha importante en el proceso de gestión de software dentro de la infraestructura tecnológica de EMAPA. Mantener sistemas obsoletos representa un riesgo crítico no solo por la exposición a ataques conocidos, sino también por el cumplimiento de normativas y estándares de seguridad. Además, el uso de versiones descontinuadas puede afectar la capacidad de integración con otros sistemas y limitar futuras actualizaciones de infraestructura. La actualización o reemplazo de esta solución debe ser tratada como una prioridad urgente.

- **21778 - IBM Lotus Domino SMTP Server Malformed Meeting Request (vCal) DoS**

Identificación

Mediante el escaneo de seguridad realizado en los servidores internos de EMAPA, se identificó una vulnerabilidad crítica asociada al servicio SMTP ejecutado por IBM

Lotus Domino. Esta debilidad fue detectada por el plugin 21778 de Nessus, el cual evidenció que la versión del servidor SMTP es susceptible a un ataque de denegación de servicio (DoS) cuando recibe solicitudes de reunión malformadas en formato vCal (vCalendar). El servicio vulnerable opera en el puerto 25/TCP.

Evaluación de riesgos

El problema identificado radica en que el componente de enrutamiento del servidor Lotus Domino consume el 100% del CPU al intentar procesar una solicitud de reunión malformada. Este fallo puede ser explotado remotamente y sin necesidad de autenticación, permitiendo a un atacante provocar la indisponibilidad completa del servicio de correo. Dado que el servidor afectado forma parte de una plataforma de mensajería corporativa, su interrupción puede tener consecuencias severas para la comunicación interna de la organización.

Impacto

Confidencialidad: Indirectamente afectada si la denegación de servicio genera desvío de información por canales inseguros.

Integridad: No se ve directamente comprometida por esta vulnerabilidad.

Disponibilidad: Totalmente comprometida, ya que un atacante puede dejar el servidor fuera de servicio simplemente con el envío de una petición malformada.

Remediación

La presente vulnerabilidad es recomendable aplicar una actualización inmediata de software donde el dominio es recomendada como la versión corregida netamente soportada en la que logra incluir 6.5.4 Fix Pack 1 y superiores a una versión de 7.0.

Mitigación

Generar una restricción de acceso hacia el puerto identificado, donde logra implementar ciertos filtros a nivel del firewall, donde se consideran en monitorear determinada alerta automática donde refleja políticas y detecciones de alta disponibilidad con el fin de recibir un impacto en cada uno de los casos de DoS.

Análisis de resultados

La presencia de esta vulnerabilidad representa una amenaza crítica para la continuidad operativa de los servicios de correo electrónico en EMAPA. El hecho de que pueda ser explotada de forma remota y sin autenticación la convierte en una debilidad de alto riesgo. Esta situación revela la importancia de mantener los sistemas actualizados y realizar auditorías periódicas que identifiquen servicios obsoletos o mal configurados. La remediación de esta vulnerabilidad debe considerarse una prioridad inmediata, tanto para preservar la disponibilidad como para fortalecer la postura general de ciberseguridad de la organización.

- **125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)**

Identificación

Se identificó una vulnerabilidad crítica asociada al protocolo Remote Desktop Protocol (RDP) sobre el puerto TCP/3389. La detección corresponde al plugin 125313 de Nessus, el cual confirma que el sistema es susceptible a la ejecución remota de código sin autenticación mediante la vulnerabilidad conocida como BlueKeep.

Esta falla, catalogada como CVE-2019-0708, permite que un atacante remoto y no autenticado ejecute instrucciones arbitrarias en el sistema objetivo. El ataque se realiza a través del envío de paquetes especialmente diseñados, lo que puede derivar en el control total del sistema vulnerable sin necesidad de generar una interacción del usuario.

Remediación

Es necesario aplicar ciertos parches de ciertos canales oficiales de la página de Microsoft, donde es necesario utilizar varios sistemas donde debe evaluar y mitigar de manera urgente las versiones modernas de soporte oficial.

Análisis de resultados

El hallazgo de BlueKeep representa una de las vulnerabilidades más críticas detectadas en la infraestructura de EMAPA. Su nivel de exposición es alarmante si se encuentra habilitado el protocolo RDP sin actualizaciones ni restricciones adecuadas.

El vector de ataque es remoto, con una puntuación CVSS v3 de 9.8, lo que lo clasifica como una amenaza de muy alto impacto. Además, esta vulnerabilidad ha sido ampliamente documentada y explotada a través de herramientas como Metasploit, Core Impact y CANVAS, lo que facilita su uso por parte de atacantes con bajo nivel técnico.

Dado que BlueKeep ha sido incorporada en listas oficiales de vulnerabilidades activamente explotadas (como las de CISA), su corrección debe considerarse una prioridad de seguridad. No aplicar los parches de manera oportuna podría comprometer seriamente la integridad de los sistemas institucionales, abriendo la puerta a ataques automatizados y campañas de ransomware.

- **53534 - IBM Lotus Domino iCalendar Email Address ORGANIZER:mailto Header Remote Overflow**

Identificación

En el servidor corporativo de EMAPA, se detectó una vulnerabilidad crítica relacionada con el servicio SMTP que corre sobre el puerto TCP/25. El escaneo arrojó que el servicio pertenece a la plataforma IBM Lotus Domino, específicamente la versión 5.0.11, la cual presenta una vulnerabilidad de desbordamiento de búfer en la cabecera de eventos iCalendar.

Esta vulnerabilidad se encuentra documentada bajo el identificador CVE-2010-3407 y corresponde al plugin 53534 de Nessus. La falla está relacionada con la ausencia de validaciones adecuadas en los límites de entrada de datos, lo cual permite que un atacante remoto provoque un desbordamiento de pila a través de mensajes SMTP especialmente diseñados.

Evaluación de riesgos

La vulnerabilidad tiene una calificación de alto riesgo debido a su capacidad para ejecutar código arbitrario de manera remota, sin requerir autenticación previa. Además, si el intento de explotación falla, puede generar condiciones de denegación de servicio (DoS), afectando la disponibilidad del servicio de correo electrónico.

El ataque se aprovecha del proceso nrouter.exe de Lotus Domino, permitiendo que el código malicioso se ejecute con los mismos privilegios del servicio comprometido, lo que puede dar paso a una toma completa del servidor afectado.

Impacto

Confidencialidad: Totalmente comprometida si se logra ejecución remota, ya que permite acceder a correos electrónicos e información sensible.

Integridad: Posibilidad de modificar, interceptar o insertar correos de forma maliciosa.

Disponibilidad: Riesgo elevado de interrupción total del servicio de correo corporativo mediante técnicas de DoS.

Remediación

Es necesario actualizar el servidor con las siguientes versiones seguras en las cuales se consideran versiones de mayor seguridad, en las cuales son las siguientes: IBM Lotus Domino 8.0.2 FP5, 8.5.1 FP2 y 8.5.2, por otra parte, se considera un desbordamiento para aplicar la actualización para eliminar el riesgo de la presente vulnerabilidad.

Mitigación

Es necesario realizar las actualizaciones del software con el objetivo de filtrar los mensajes SMTP que contengan cabeceras iCalendar mal formadas, también es necesario imitar ciertos accesos hacia el puerto 25 con las configuraciones de direcciones IPs realmente confiables dentro de la red corporativa. Finalmente es necesario monitorear una actividad de búsqueda inusual.

Análisis de resultados

Esta vulnerabilidad es especialmente preocupante porque afecta un sistema crítico para las comunicaciones internas y externas de EMAPA. La versión del servicio identificado, Lotus Domino 5.0.11, es considerablemente antigua y se encuentra fuera del soporte oficial, lo que agrava el riesgo.

Al tener una puntuación CVSS de 9.3, esta vulnerabilidad representa una amenaza inmediata, que puede ser fácilmente aprovechada por un atacante con conocimientos básicos y acceso a herramientas como Metasploit, CANVAS o Core Impact.

La prioridad es alta: debe actualizarse el software o considerarse una migración hacia una plataforma más moderna y con soporte activo. Mantener esta versión expone a la organización a posibles filtraciones de información, interrupciones de servicio o compromisos del servidor de correo.

- **152102 - Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)**

Identificación

Los servicios accesibles en la red interna de EMAPA, se detectó una vulnerabilidad de escalamiento de privilegios en el servicio CIFS (Common Internet File System), que opera sobre el puerto TCP/445. Esta vulnerabilidad está identificada como PetitPotam y registrada con el número CVE-2021-36942. Se trata de una debilidad en el protocolo EFSRPC (Encrypting File System Remote Protocol), la cual puede ser explotada de forma remota y sin autenticación previa.

La prueba realizada a través de la herramienta de escaneo Nessus evidenció que el servidor es vulnerable al envío de peticiones EFSRPC especialmente diseñadas, que provocan una conexión forzada del servidor víctima hacia un recurso remoto controlado por un atacante. Esta conexión es el punto de partida para un relay de autenticación NTLM, lo que permite al atacante suplantar la identidad del host víctima y autenticarse en otros sistemas de la red.

Evaluación de riesgos

Aunque esta vulnerabilidad no permite ejecución directa de código, representa una amenaza crítica para la seguridad interna del dominio, especialmente en entornos con servicios como Active Directory Certificate Services (AD CS) mal configurados. Si se logra completar el ataque, el atacante podría obtener un certificado de autenticación válido como un controlador de dominio, permitiendo así el movimiento lateral y comprometiendo completamente el dominio de Windows.

Impacto

Confidencialidad: Comprometida si se logra acceso a servicios autenticados bajo la identidad del servidor víctima.

Integridad: Peligro de acciones no autorizadas en recursos internos de la red.

Disponibilidad: No se ve directamente afectada, pero la cadena de ataque posterior puede derivar en impactos graves.

Remediación

Es necesario aplicar actualizaciones, donde tiene un acuerdo con las guías de fabricantes del respectivo archivo, por otro lado, genera una revisión en la que es necesario deshabilitar la autenticación NTLM con ciertos filtros RPC con el objetivo de bloquear ciertos accesos remotos en ciertas interfaces UUIS, donde generalmente implementan las políticas en los certificados de los entornos con AD y CS.

Mitigación

Es fundamental restringir el acceso al puerto 445 desde que son las redes confiables, por otro lado, es necesario monitorear varios controladores de seguridad donde busca los intentos de conectividad para evaluar varios usos de las herramientas RpcFirewall para filtrar y visualizar el protocolo EFSRPC.

Análisis de resultados

La detección de PetitPotam dentro de la infraestructura representa un punto de entrada sumamente peligroso para un atacante con conocimientos medios. Al no requerir credenciales para su ejecución inicial, puede ser el primer paso para comprometer todo el dominio si se combina con otros vectores, como un servidor AD CS mal protegido.

Con una puntuación CVSS v3.0 de 7.5 y una probabilidad de explotación muy alta (EPSS 0.9353), esta amenaza debe ser tratada con alta prioridad, especialmente en redes internas que utilicen autenticación NTLM o certificados digitales.

- **26920 - SMB NULL Session Authentication**

Identificación

El protocolo SMB (Server Message Block) en uno de los servidores internos de EMAPA, se identificó una grave vulnerabilidad que permite autenticación mediante sesiones NULL, es decir, sin necesidad de ingresar un nombre de usuario ni contraseña. Esta debilidad está clasificada como SMB NULL Session Authentication y corresponde a los CVE-1999-0519, CVE-1999-0520 y CVE-2002-1117.

La sesión NULL permite que un atacante remoto no autenticado se conecte a ciertos recursos compartidos del sistema, como los pipes browser o spoolss, accediendo potencialmente a información sensible del sistema operativo, usuarios, servicios y configuraciones de red.

Evaluación de riesgos

Este tipo de vulnerabilidad representa un riesgo elevado debido a que permite la enumeración remota de información sin necesidad de autenticación, donde es necesario recolectar la información, para identificar y planifica ciertos movimientos en varios escalamientos de privilegios.

Impacto

Confidencialidad: Comprometida, al permitir la exposición de información interna sin autenticación.

Integridad: Potencialmente vulnerable si se accede a recursos mal configurados.

Disponibilidad: En menor medida, pero puede ser afectada si se abusa de recursos compartidos o se desencadenan errores.

Remediación

Esta presente vulnerabilidad forma parte de una mala configuración del servicio SMB y es necesario deshabilitar completamente las sesiones identificadas como NULL, con ciertas claves de registro para los sistemas afectados, donde tambien es necesario aplicar las políticas del grupo para evitar un acceso anónimo con los recursos compartidos, actualizar el sistema operativo y finalmente monitorear las conexiones para una revisión del firewall para detectar las actividades de alertas sospechosas.

Mitigación

Esto se ejecuta para filtrar ciertos accesos hacia el puerto 445 donde se proporcionan desde la red externa, donde no son confiables, para revisar ciertos permisos de los recursos compartidos, en el cual se identifique usuarios anónimos.

En este caso es primordial deshabilitar SMBv1 donde se presenta múltiples vulnerabilidades con un historio definido para aplicar cambios definidos.

Análisis de resultados

La presencia de esta vulnerabilidad demuestra una configuración heredada o desactualizada del servicio SMB. En el contexto actual, donde se prioriza el principio de mínimo privilegio, permitir autenticación sin credenciales representa un riesgo inaceptable. Además, este tipo de sesiones puede ser aprovechado por scripts automatizados o herramientas como enum4linux y Metasploit, facilitando significativamente la fase de reconocimiento de un atacante.

Resumen de los 20 Servidores Virtualizados en la Matriz de Riesgo

Servidor	Críticas	Altas	Medias	Bajas	Total Vulnerabilidades	Clasificación de Riesgo
Servidor de Correo	2	1	2	0	5	Crítico
Servidor SGBD Documental	1	1	2	0	4	Alto
Servidor Comercial	2	1	2	0	5	Crítico
Servidor BD Comercial	1	1	2	1	5	Alto
Servidor Administrativo	2	2	3	1	8	Crítico
Servidor Dominio EMAPA	2	2	3	0	7	Crítico
Servicios en Línea	2	1	2	1	6	Crítico
Servidor Antivirus	2	1	3	0	6	Crítico
Servidor Registros Asistencia	2	1	2	0	5	Crítico
Servidor Help Desk	0	0	1	1	2	Bajo
Servidor Cliente GIS	0	0	1	1	2	Bajo
Servidor Aplicaciones EMAPA	2	2	2	0	6	Crítico
Servidor Documental	2	2	2	0	6	Crítico
Servidor Licencias WSCAD	1	1	2	0	4	Alto
Servidor Financiero Antiguo	2	2	2	0	6	Crítico
Servidor Desarrollo	1	1	1	1	4	Alto
Servidor BD Servicios en Línea	2	1	1	0	4	Crítico
Servidor Comercial (2)	1	1	2	0	4	Alto
Servidor Registros	2	2	2	0	6	Crítico
Servidor de Seguridad	2	2	3	0	7	Crítico

Figura 33. Matriz de riesgo asado en la Norma ISO 31000

3.3 Estadísticas de Criticidad de las herramientas Nessus, Nmap y OpenVas

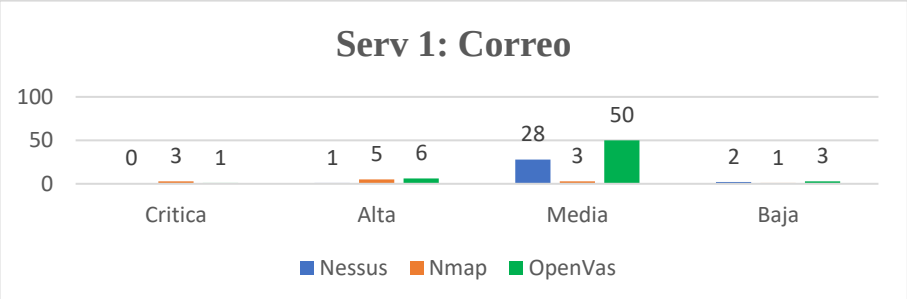


Figura 34. Criticidad media en Servidor 1 Correo con OpenVas

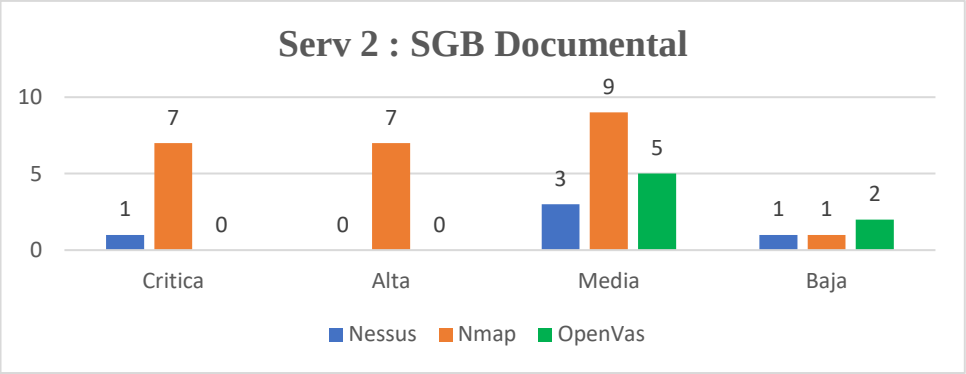


Figura 35. Criticidad media en Servidor 2 SGBD Documental con Nmap

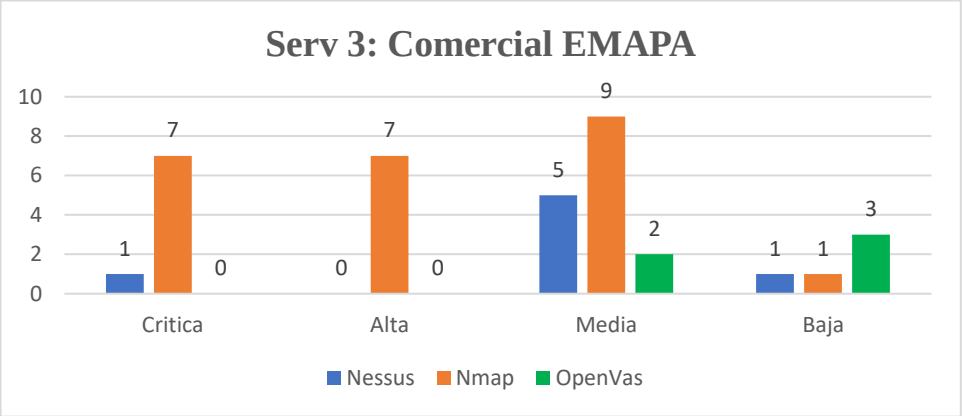


Figura 36. Criticidad media en Servidor 3 Comercial EMAPA con Nmap

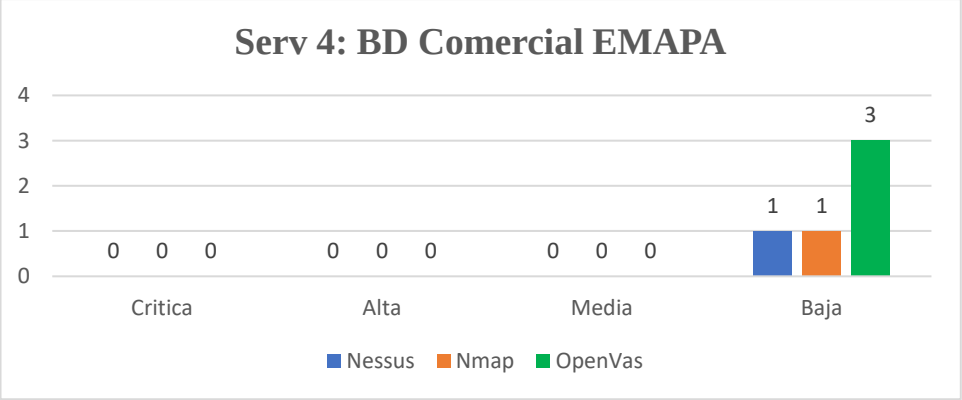


Figura 37. Criticidad baja en Servidor 4 BD Comercial EMAPA con OpenVas

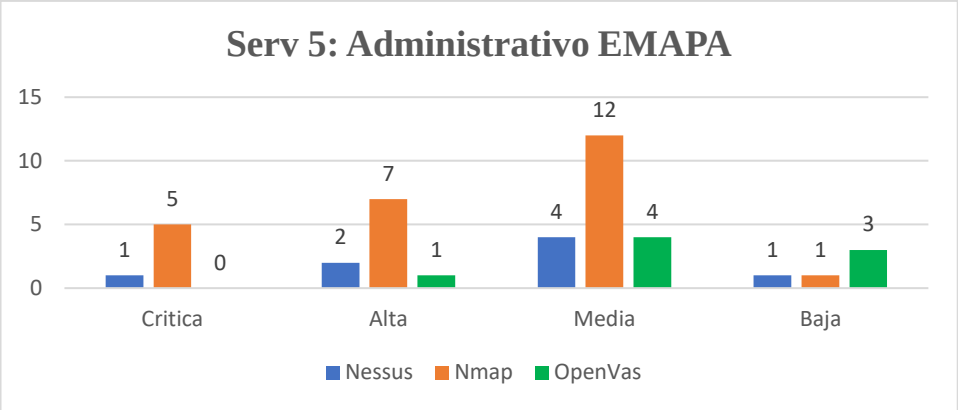


Figura 38. Criticidad media en Servidor 5 Administrativo EMAPA con Nmap

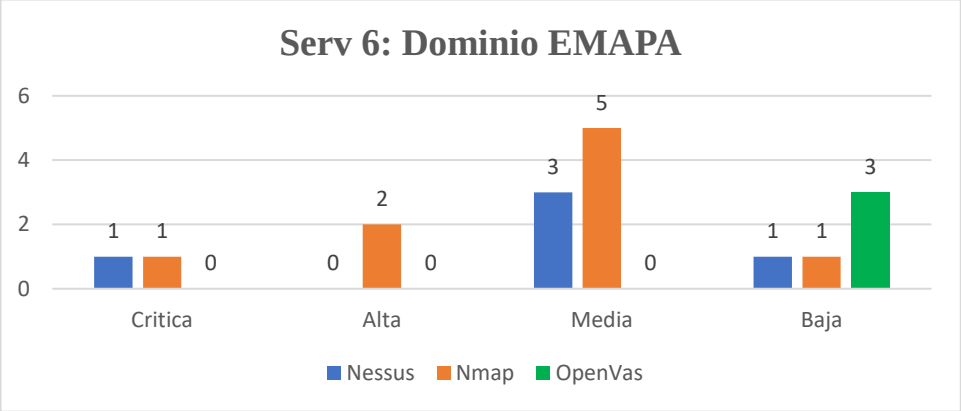


Figura 39. Criticidad media en Servidor 6 Dominio con Nmap

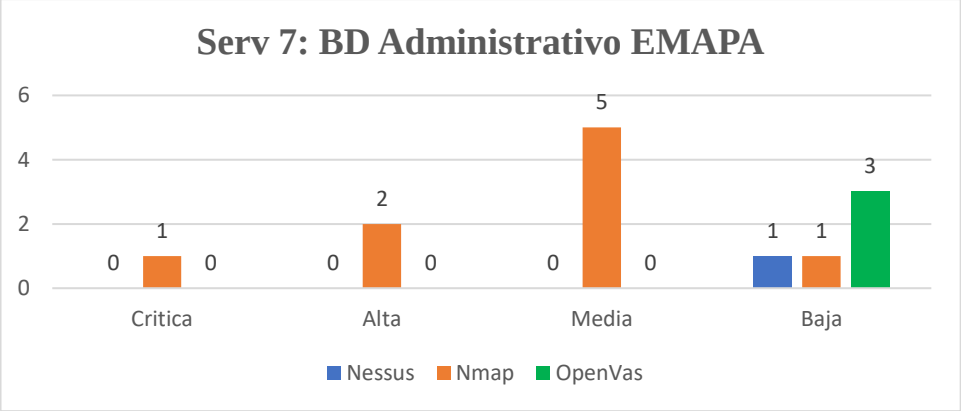


Figura 40. Criticididad media en Servidor 7 BD Administrativo con Nmap

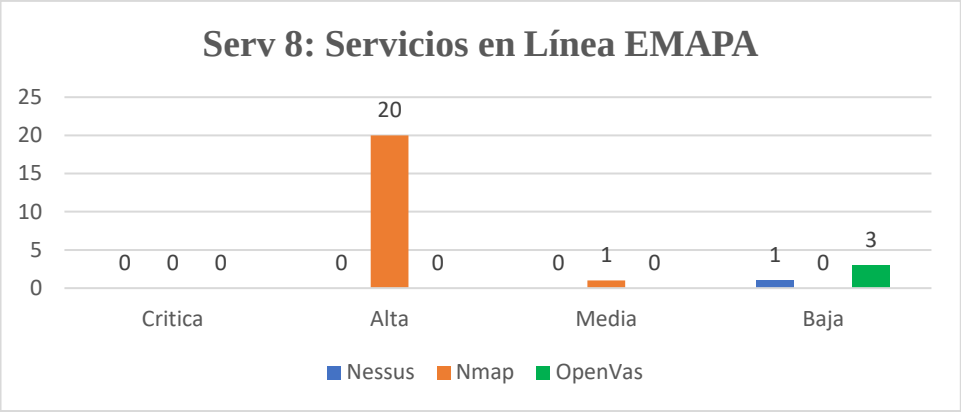


Figura 41. Criticidad alta en Servidor 8 Servicios en Línea EMAPA con Nmap

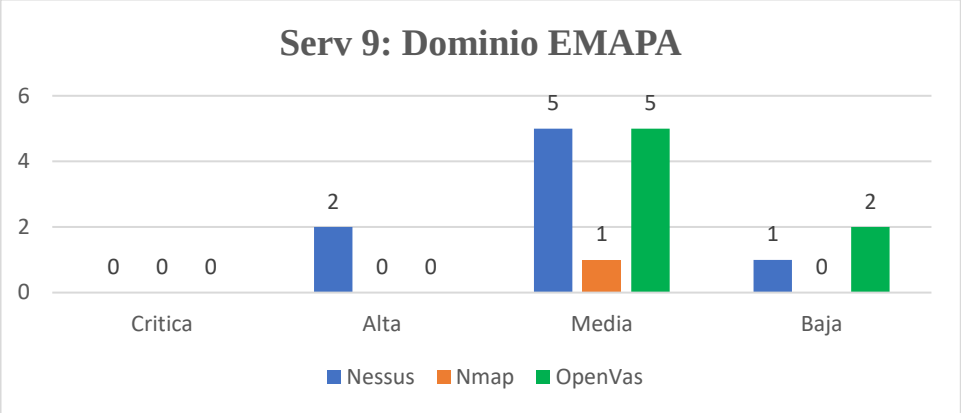


Figura 42. Criticidad media en Servidor 9 Dominio con Nessus y OpenVas

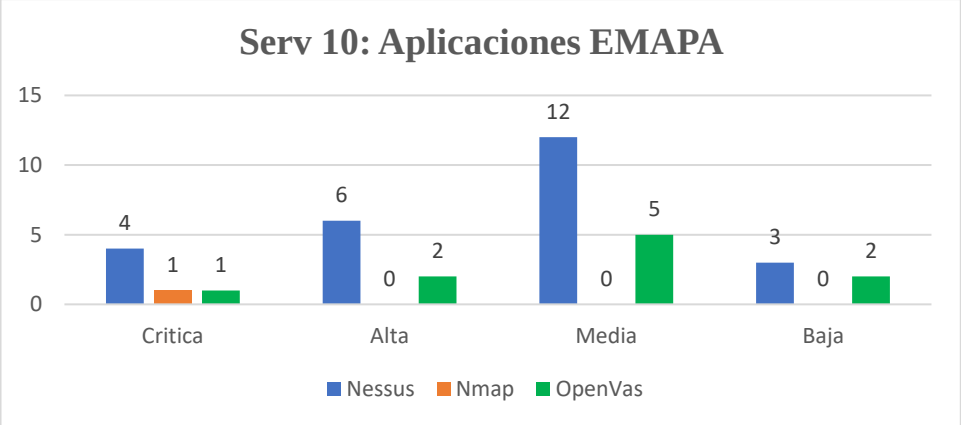


Figura 43. Criticidad media en Servidor 10 Aplicaciones con Nessus

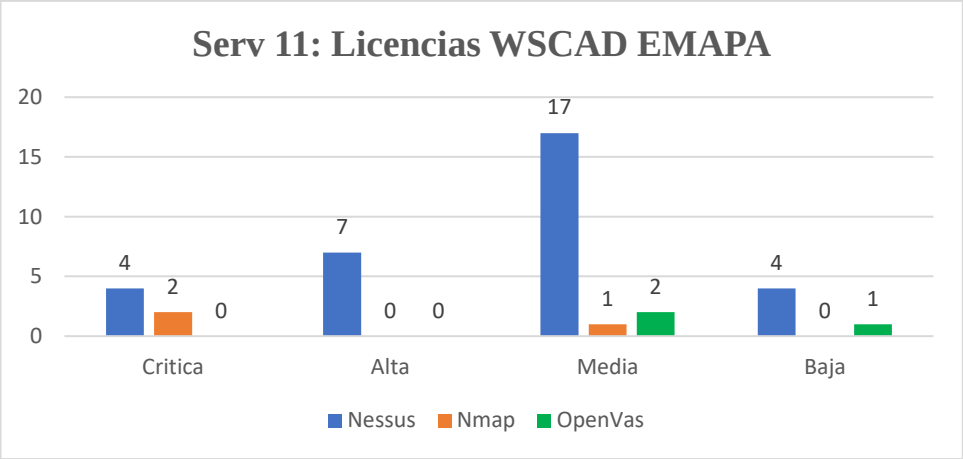


Figura 44. Criticidad media en Servidor 11 Licencias WSCAD con Nessus

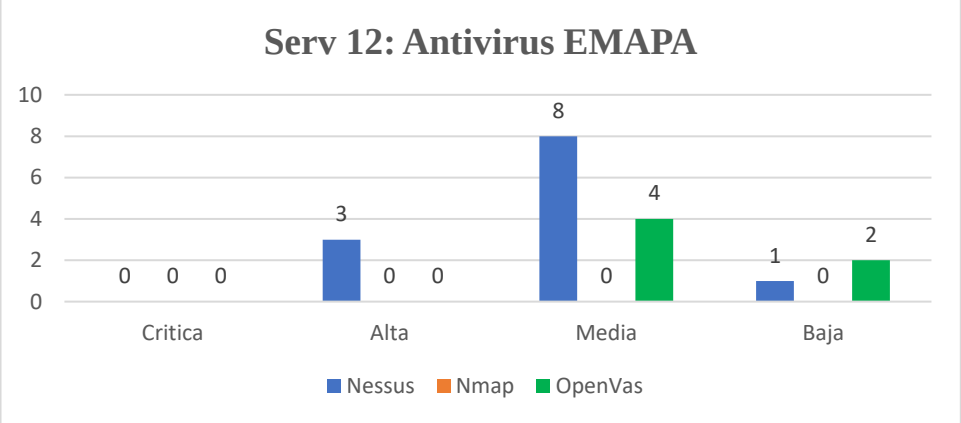


Figura 45. Criticidad media en Servidor 12 Antivirus con Nessus

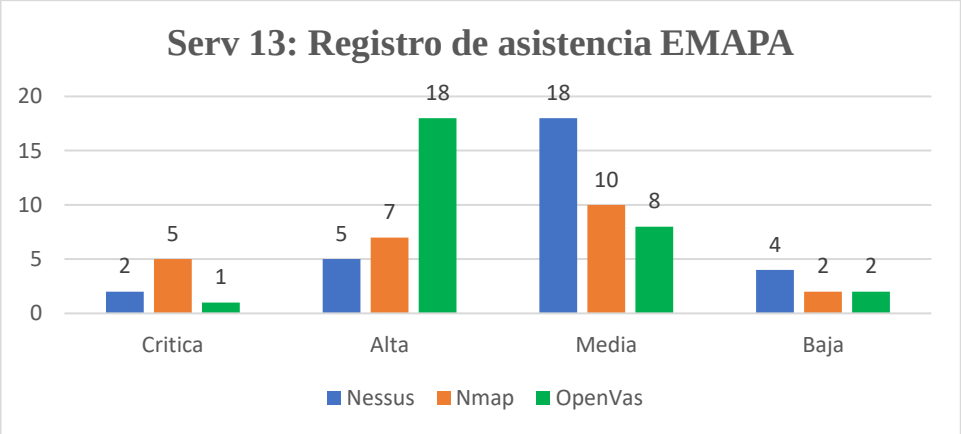


Figura 46. Criticidad alta y media en Servidor 13 Registro de asistencia con Nessus y OpenVas

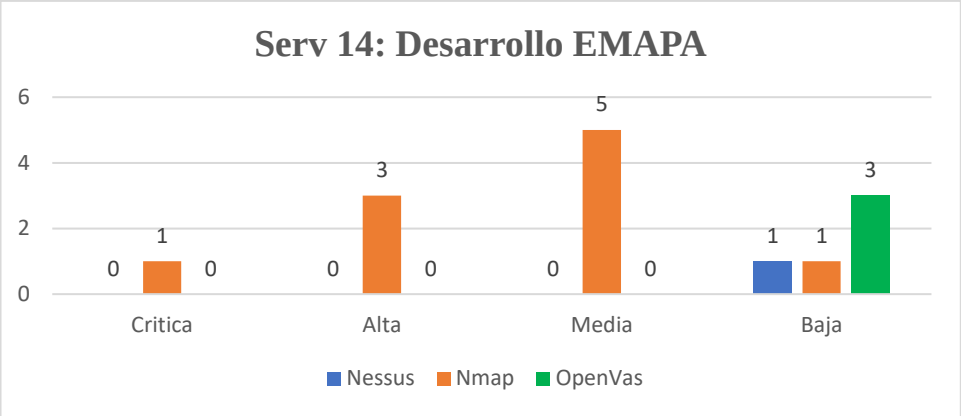


Figura 47. Criticidad media en Servidor 14 Desarrollo con Nmap

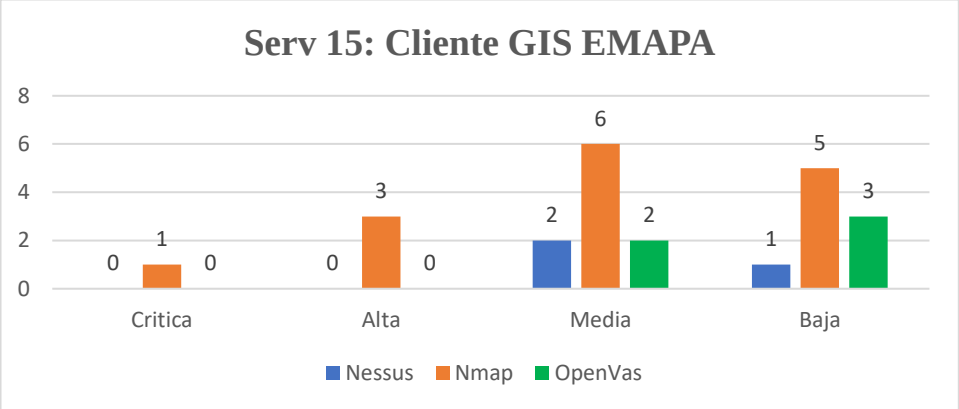


Figura 48. Criticidad media en Servidor 15 Cliente GIS con Nmap

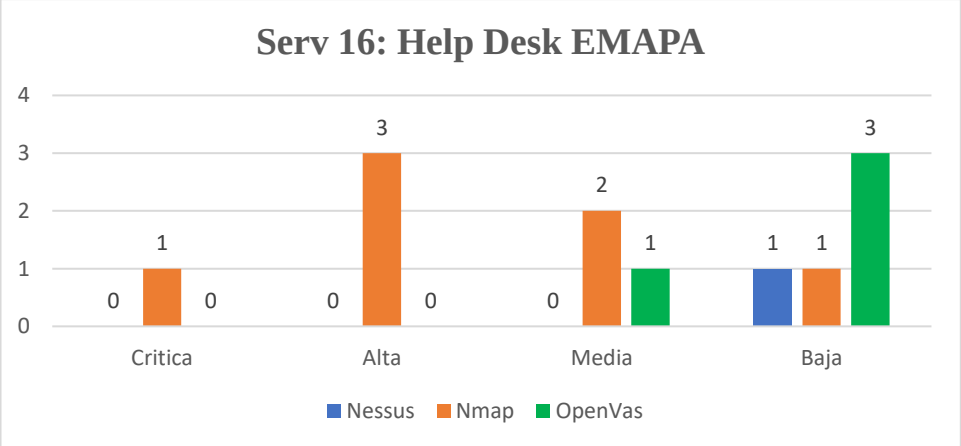


Figura 49. Criticidad alta y baja en Servidor 16 Help Desk con Nmap y OpenVas

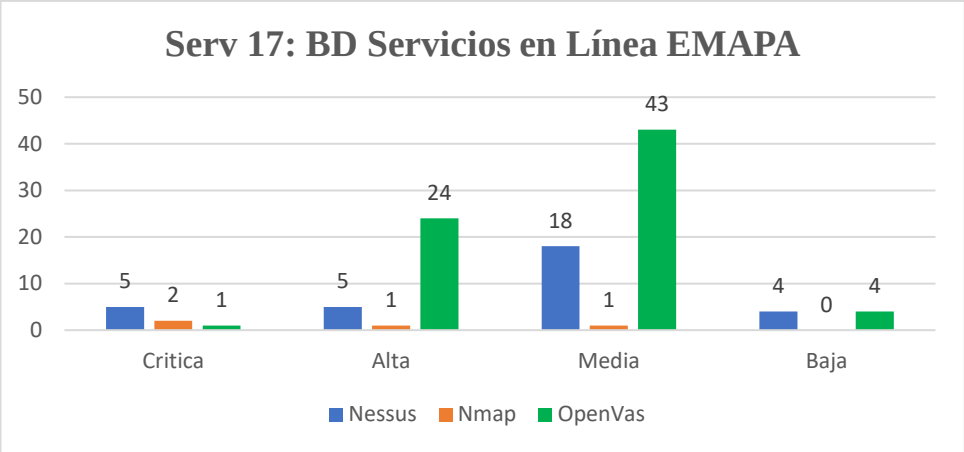


Figura 50. Criticidad alta y media en Servidor 17 BD Servicios en Línea con OpenVas

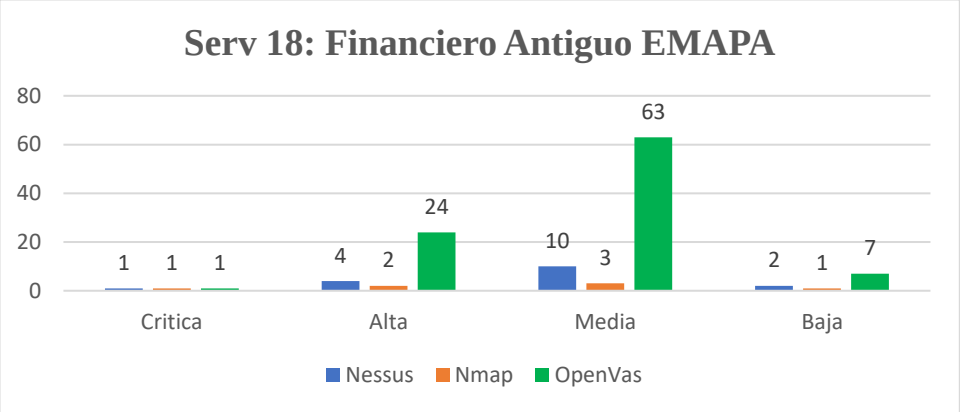


Figura 51. Criticidad media en Servidor 18 Financiero Antiguo con OpenVas

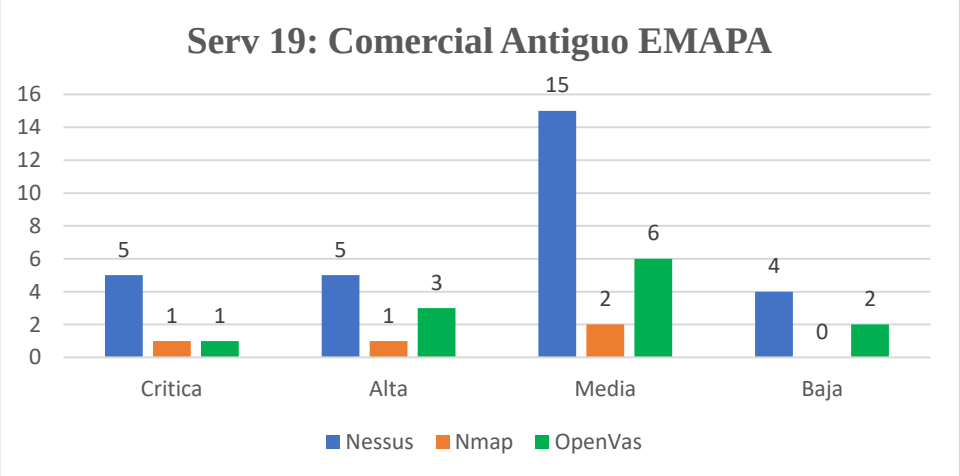


Figura 52. Criticidad media en Servidor 19 Comercial Antiguo con Nessus

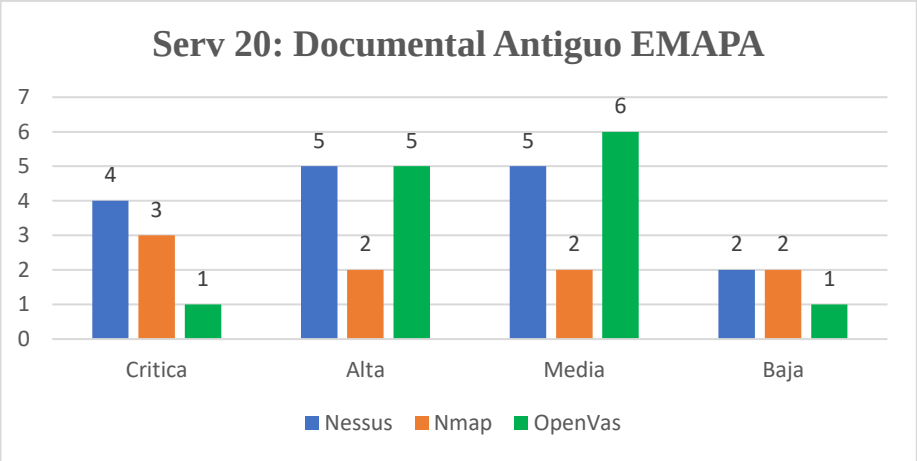


Figura 53. Criticidad Servidor 20 Documental Antiguo

3.4 Entrega del Informe a Jefatura de TI de la empresa EMAPA

Esta parte se logra presentar a continuación el informe detallado de las vulnerabilidades de los servidores internos de la empresa EMAPA para el Jefe de Tecnologías de la información, en el siguiente enlace: Ver informe en PDF.

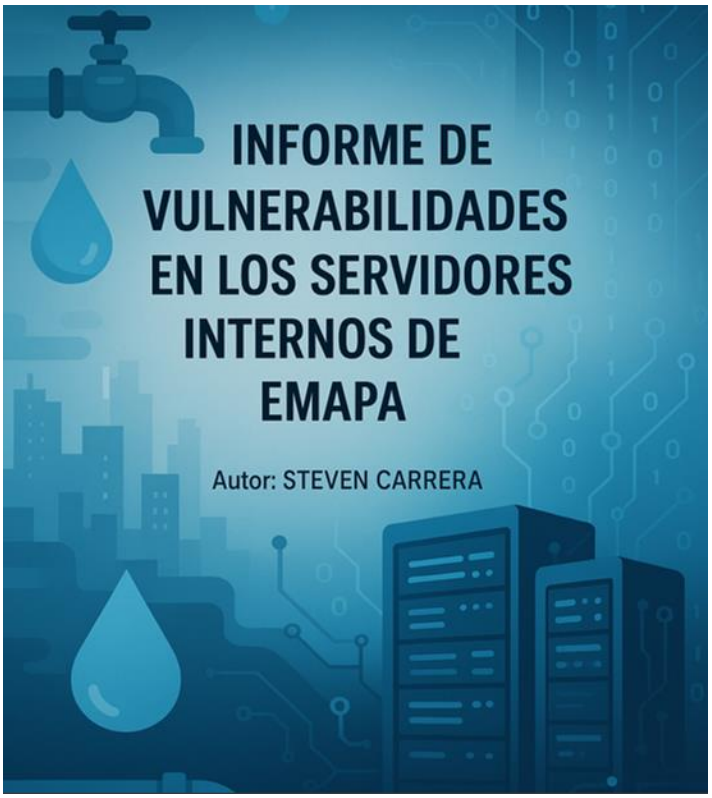


Figura 54. Portada del Informe de Vulnerabilidades Jefe de TI

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- A lo largo de esta investigación se evidenció que los servidores internos de la empresa EMAPA presentan diversas vulnerabilidades que, de no ser atendidas, pueden afectar directamente la continuidad operativa, la disponibilidad de los servicios y la integridad de los datos institucionales. Este análisis permitió identificar los puntos más críticos de exposición y establecer una base para la toma de decisiones técnicas orientadas a mejorar la seguridad informática.

- Mediante el uso de herramientas especializadas como Nessus, Nmap y OpenVAS, se logró realizar un análisis detallado de las vulnerabilidades presentes, clasificándolas por nivel de criticidad. Esto facilitó la priorización de las amenazas que requieren atención inmediata, además de validar la efectividad de estas herramientas en entornos reales de producción.

- El enfoque metodológico aplicado permitió cumplir con los objetivos establecidos, proporcionando un diagnóstico técnico fundamentado sobre el estado de los servidores. Esta información resulta clave para la implementación de planes de mejora continua en la gestión de la seguridad informática de EMAPA.

- La identificación de vulnerabilidades como protocolos obsoletos, configuraciones inseguras y servicios desactualizados demuestra la necesidad de establecer controles preventivos y correctivos permanentes. Asimismo, el trabajo puso en evidencia la falta de procedimientos estandarizados para el monitoreo y evaluación periódica de riesgos tecnológicos.

- Finalmente, este proyecto de investigación deja un concepto claro que el fortalecimiento de la seguridad informática no solo es una necesidad técnica, sino también una responsabilidad estratégica que incide directamente en la confiabilidad institucional y en la protección de la información crítica de la empresa.

4.2 Recomendaciones

- Se recomienda establecer un plan de gestión de vulnerabilidades, con escaneos periódicos y actualizaciones constantes, que incluya políticas de mantenimiento, revisión de configuraciones críticas y aplicación de parches de seguridad conforme a las mejores prácticas del sector.

- Es fundamental mantener un inventario actualizado de hardware y software, junto con una bitácora técnica que registre cada modificación realizada en los sistemas, incluidas actualizaciones de sistema operativo, firmware y componentes de red.

- Se sugiere implementar capacitaciones regulares para el personal del área de TI, orientadas al uso de herramientas de análisis de vulnerabilidades, buenas prácticas de seguridad, y respuesta ante incidentes informáticos.

- Se recomienda migrar servicios y sistemas que operan sobre plataformas obsoletas o sin soporte a versiones modernas que cuenten con mantenimiento activo por parte del fabricante, garantizando así una protección efectiva frente a amenazas emergentes.

- Es necesario reforzar la configuración de protocolos de comunicación seguros, especialmente en servicios que utilizan SSL/TLS, deshabilitando algoritmos de cifrado débiles y configurando suites criptográficas fuertes y actualizadas.

- Se sugiere incorporar servidores redundantes o esquemas de alta disponibilidad, con el fin de asegurar la continuidad operativa ante fallos del sistema principal. Esto es especialmente crítico para los servicios que respaldan procesos operativos esenciales de EMAPA.

- Por último, se recomienda que la empresa establezca un comité técnico de seguridad informática que evalúe periódicamente los riesgos, revise los informes de escaneo y proponga acciones de mejora continua orientadas a reducir la superficie de ataque de la infraestructura tecnológica.

REFERENCIAS BIBLIOGRÁFICAS

[1] A. Smith, B. Jones, y C. Thompson, "Cybersecurity Standards and Frameworks for Public Sector," IEEE Security & Privacy, vol. 19, no. 6, pp. 34–40, 2021.

[2] L. Martínez, "Ciberseguridad en servicios públicos: Desafíos y oportunidades en América Latina," IEEE Latin America Transactions, vol. 20, no. 4, pp. 1203–1210, 2022.

[3] J. Pérez y M. Gómez, "Análisis de vulnerabilidades en infraestructura tecnológica de servicios públicos," IEEE Computer Society, vol. 15, no. 2, pp. 72–78, 2023.

[4] M. Gómez y D. Sánchez, "Auditoría de seguridad informática: Estrategias y mejores prácticas en empresas públicas," IEEE Trans. Inf. Forensics Security, vol. 19, no. 1, pp. 10–16, 2024.

[5] J. Smith y A. Lopez, "Information Security Audits in Latin America: Methodologies and Impact," IEEE Trans. Inf. Forensics Security, vol. 15, no. 3, pp. 1234–1245, Mar. 2020.

[6] K. Patel y M. Zhang, "Vulnerability Assessment Frameworks for IT Infrastructure: A Comparative Analysis," IEEE Access, vol. 8, pp. 98765–98780, Jun. 2021.

[7] R. Johnson et al., "Cybersecurity Vulnerability Management in Organizational Networks," IEEE Security & Privacy, vol. 18, no. 2, pp. 52–60, Apr. 2022.

[8] L. Torres y P. Hansen, "Security Audits in Server Environments: An Automated Approach," IEEE Syst. J., vol. 13, no. 1, pp. 456–465, Jan. 2019.

[9] D. Nguyen y G. Rodriguez, "Impact of Vulnerabilities on Information Systems: Case Studies and Mitigation Strategies," IEEE Comput. Soc., vol. 20, no. 5, pp. 38–47, May 2023.

[10] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization, Geneva, Switzerland, 2013.

[11] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Gaithersburg, MD, USA, Apr. 2018.

[12] FIRST.org, Inc., Common Vulnerability Scoring System (CVSS), Version 3.1, Jun. 2019. [Online]. Available: https://www.first.org/cvss

[13] L. García y R. Sánchez, Auditoría y Seguridad Informática: Conceptos, Técnicas y Herramientas. México: Alfaomega, 2021.

[14] M. Bishop, Introduction to Computer Security. Boston, MA, USA: Addison-Wesley, 2004.

[15] D. Gollmann, Computer Security, 3rd ed. Chichester, West Sussex, UK: Wiley, 2011.

[16] IETF, RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280

[17] Mozilla, Server Side TLS: Guidelines, Mozilla Wiki, 2024. [Online]. Available: https://wiki.mozilla.org/Security/Server_Side_TLS

[18] SSL Labs, SSL Server Test, Qualys. [Online]. Available: https://www.ssllabs.com/ssltest/

[19] OpenSSL Project, OpenSSL Security Advisory [24 August 2016]: SWEET32 Vulnerability, 2016. [Online]. Available: https://www.openssl.org/blog/blog/2016/08/24/sweet32/

[20] Karthikeyan Bhargavan and Gaëtan Leurent, SWEET32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN, INRIA, 2016. [Online]. Available: https://sweet32.info

[21] Python Software Foundation, Python Release Cycle, Python Developer's Guide. [Online]. Available: https://devguide.python.org/devcycle/

[22] Python Software Foundation, Download Python, 2024. [Online]. Available: https://www.python.org/downloads/

[23] NIST, CVE-2021-3177: Python buffer overflow vulnerability, NVD. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-3177

[23] CVE-1999-0524, ICMP Timestamp Request Remote Date Disclosure, NIST NVD. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-1999-0524

[24] OWASP, ICMP-based vulnerabilities, OWASP Foundation. [Online]. Available: https://owasp.org/www-community/attacks/ICMP_Injection

[25] Cisco, ICMP Best Practices, Cisco Documentation. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/internet-control-message-protocol-icmp/20007-icmp.html

[26] NIST, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, Special Publication 800-40 Rev. 3, 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[27] OWASP Foundation, Top 10 Security Risks, OWASP, 2023. [Online]. Available: https://owasp.org/www-project-top-ten/

[28] ISO/IEC 27001, Information Security Management Systems Requirements, International Organization for Standardization, 2013.

[29] Tenable, Inc., *Nessus Professional: Data Sheet*. Columbia, MD, USA: Tenable Network Security, 2023. [Online]. Available: https://www.tenable.com/products/nessus

[30] A. Scarfone y M. Mell, "Guide to Vulnerability Assessment," *NIST Special Publication 800-115*, National Institute of Standards and Technology, Gaithersburg, MD, USA, Sep. 2008. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-115/final

[31] G. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. USA: Insecure.Com LLC, 2009.

[32] Greenbone AG, *Greenbone OpenVAS Overview: Security Feed and Vulnerability Management*, 2023. [Online]. Available: https://www.greenbone.net/en/product/greenbone-vulnerability-management/

[33] P. Grayson, K. Brune, y R. M. Smith, "Comparative Study of Vulnerability Scanners: Nessus, OpenVAS and Nexpose," *Int. J. of Computer Applications*, vol. 173, no. 10, pp. 1–6, Sep. 2017.

[34] A. Behal, K. Kumar, y M. Sachdeva, "Network vulnerability assessment using open source tools," *Procedia Computer Science*, vol. 85, pp. 702–710, 2016.

[35] M. I. Sharif, A. W. Malik, y S. A. Khayam, "A Comparative Study of Network Security Tools for Vulnerability Assessment," *IEEE Secur. Priv.*, vol. 13, no. 3, pp. 74–79, May 2015.

ANEXOS

Anexo A. Instalación de Nessus en AlmaLinux

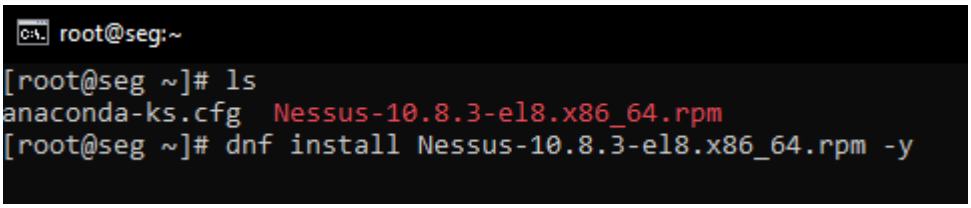


Figura 55. Instalación AlmaLinux en la consola de AlmaLinux

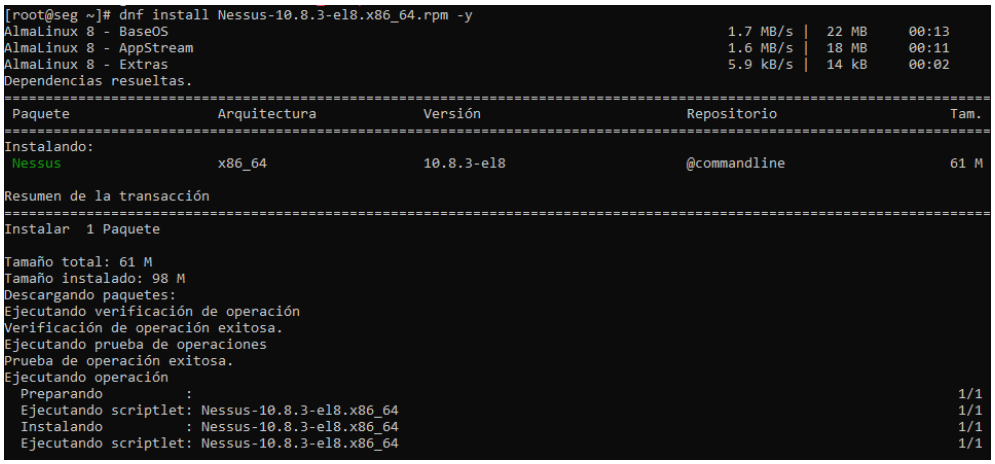


Figura 56. Paquetes descargados desde Almalinux

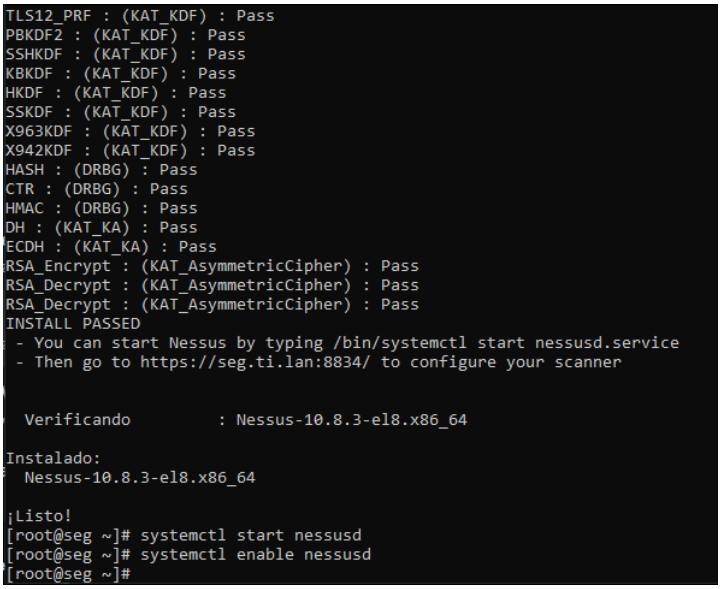


Figura 57. Inicilización del servicio de Nessus

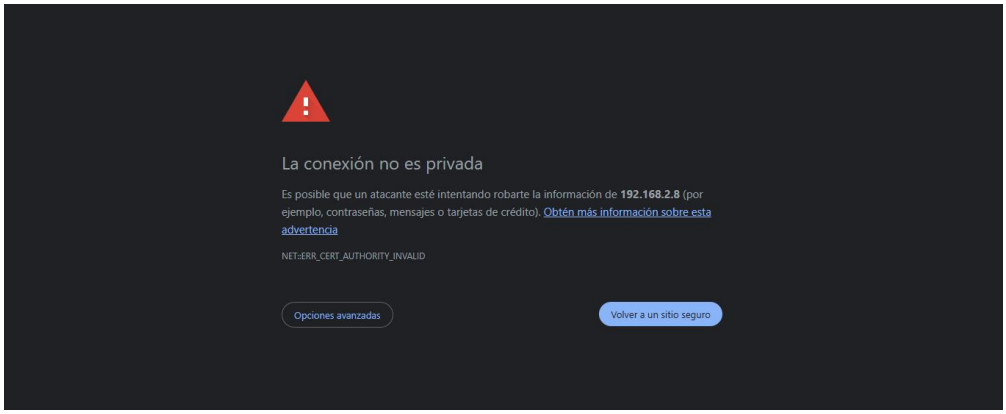


Figura 58. Ingreso con la IP de la herramienta Nessus en el navegador

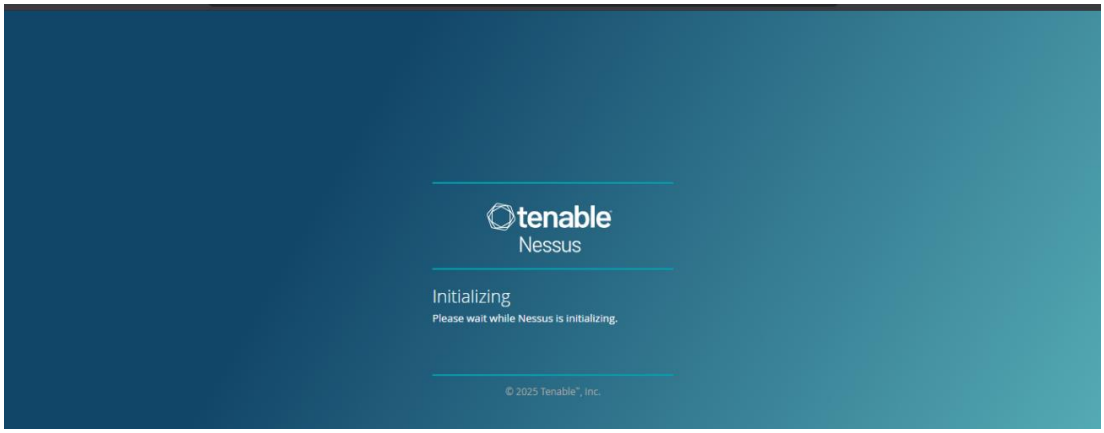


Figura 59. Interfaz de la Inicialización de la herramienta de Nessus

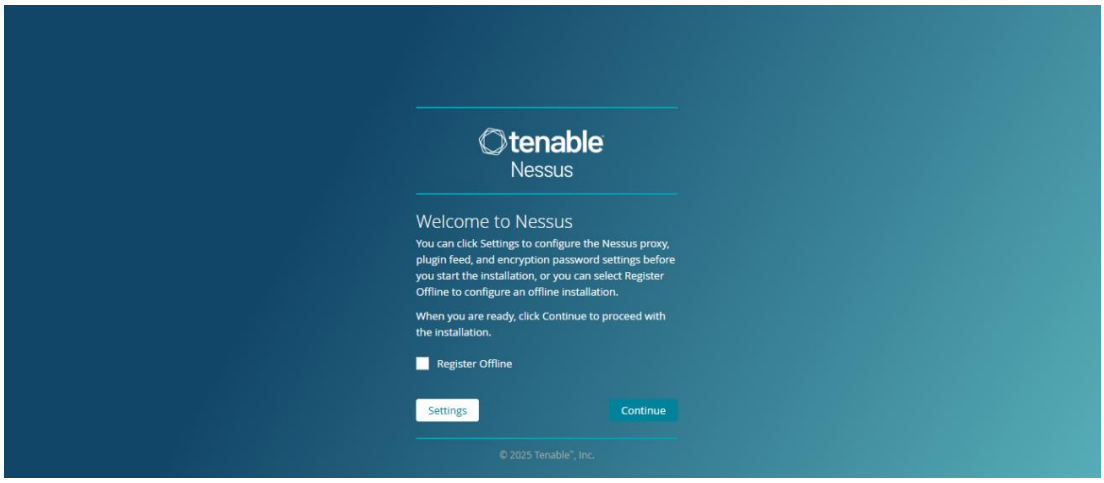


Figura 60. Plataformas de bienvenida para aceptar el registro

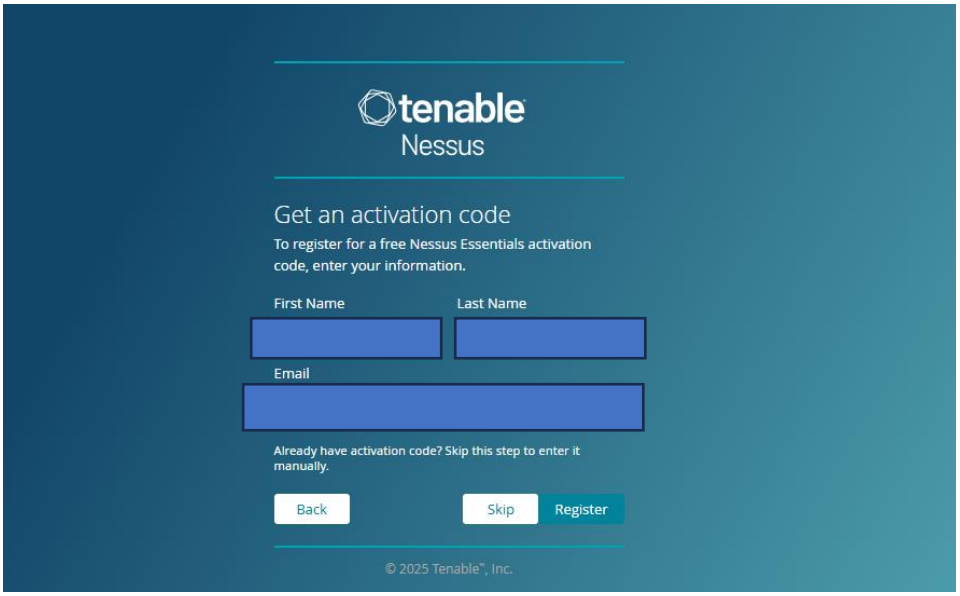


Figura 61. Platafoma de registro en la herramienta de Nessus

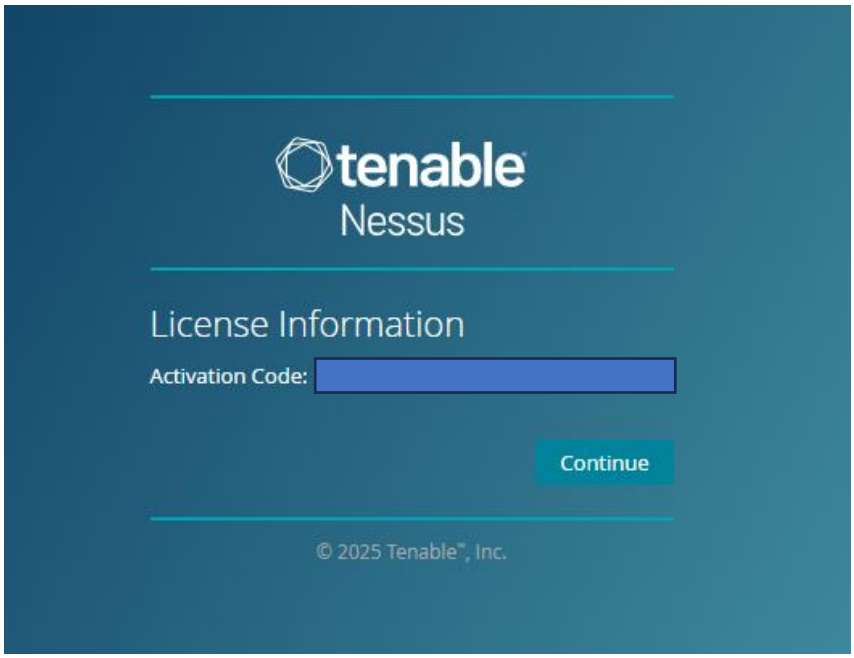


Figura 62. Código de activación

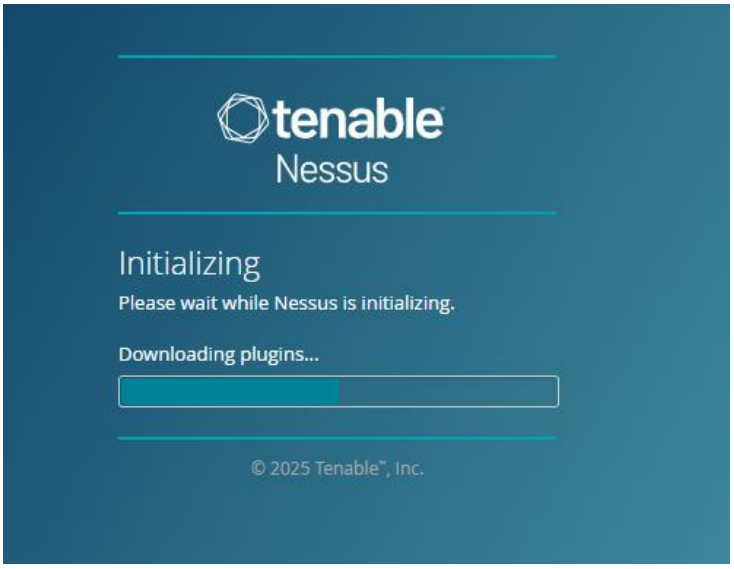


Figura 63. Descarga de los plugins

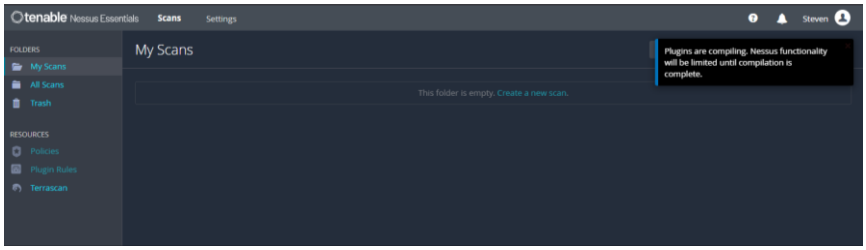


Figura 64. Interfaz de Nessus para lo su utilidad

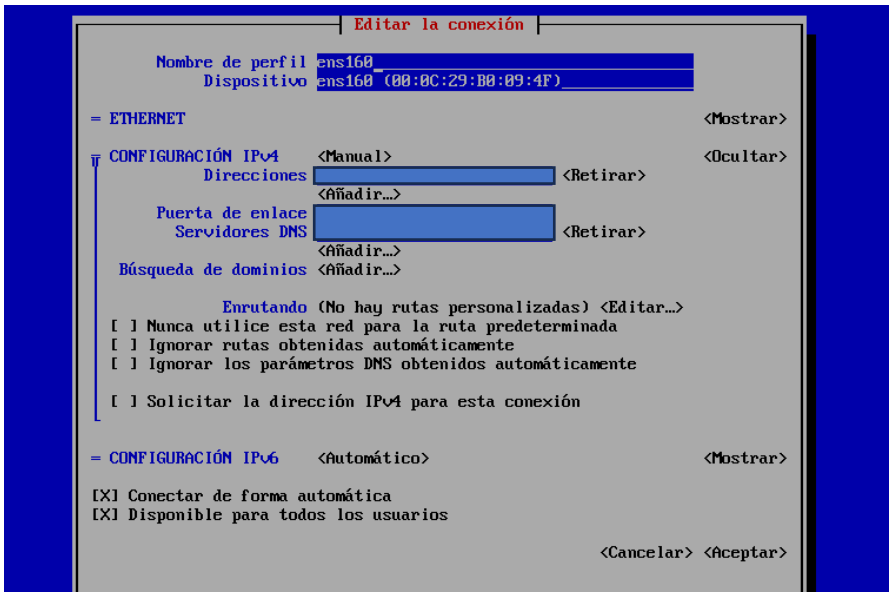


Figura 65. Configuración de la IP estática

Anexo B. Plantilla Matriz de Riesgo

Servidor	Criticas	Altas	Medias	Bajas	Total Vulnerabilidades	Clasificación de Riesgo
Servidor de Correo	2	1	2	0	5	Critico
Servidor SGBD Documental	1	1	2	0	4	Alto
Servidor Comercial	2	1	2	0	5	Critico
Servidor BD Comercial	1	1	2	1	5	Alto
Servidor Administrativo	2	2	3	1	8	Critico
Servidor Dominio EMAPA	2	2	3	0	7	Critico
Servicios en Linea	2	1	2	1	6	Critico
Servidor Antivirus	2	1	3	0	6	Critico
Servidor Registros Asistencia	2	1	2	0	5	Critico
Servidor Help Desk	0	0	1	1	2	Bajo
Servidor Cliente GIS	0	0	1	1	2	Bajo
Servidor Aplicaciones EMAPA	2	2	2	0	6	Critico
Servidor Documental	2	2	2	0	6	Critico
Servidor Licencias WSCAD	1	1	2	0	4	Alto
Servidor Financiero Antiguo	2	2	2	0	6	Critico
Servidor Desarrollo	1	1	1	1	4	Alto
Servidor BD Servicios en Linea	2	1	1	0	4	Critico
Servidor Comercial (2)	1	1	2	0	4	Alto
Servidor Registros	2	2	2	0	6	Critico
Servidor de Seguridad	2	2	3	0	7	Critico

Matriz de Riesgo | Resumen Estadístico

Figura 66. Plantilla de Excel Matriz de Riesgo

Nivel de Criticidad	Cantidad
Criticas	20
Altas	15
Medias	23
Bajas	6
Total	64

Critico	
Alto	
Bajo	

Matriz de Riesgo | Resumen Estadístico

Figura 67. Plantilla de Excel Resumen Estadístico