ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y EDUCACIÓN CONTINUA

INFORME DEL PROYECTO DE TITULACIÓN

PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN CIBERSEGURIDAD

MODALIDAD:

PROYECTO DE TITULACIÓN

TEMA:

SISTEMA DE CIBERSEGURIDAD MEDIANTE BIBLIOTECA DE CÓDIGO ABIERTO EN LOS SERVIDORES DE LOS HOSPITALES DEL IESS PROVINCIA DE MANABÍ

AUTORES:

ING. CRISTHIAN JAVIER CEDEÑO MOSQUERA

ING. ELBERTH CECILIO RIVERO GARCÍA

TUTOR:

ING. NÉSTOR ADRIÁN MORA MACÍAS, Mg.

CALCETA, JULIO 2023

DERECHOS DE AUTORÍA

CRISTHIAN JAVIER CEDEÑO MOSQUERA y ELBERTH CECILIO RIVERO GARCÍA, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, que se han respetado los derechos de autor de terceros, por lo que asumimos la responsabilidad sobre el contenido del mismo, así como ante la reclamación de terceros, conforme a los artículos 4, 5 y 6 de la Ley de Propiedad Intelectual.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido en el artículo 46 de la Ley de Propiedad Intelectual y su Reglamento.

Firmado electrónicamente por:
CRISTHIAN JAVIER CEDENO MOSQUERA

Firmado electrónicamente por:
ELBERTH CECILIO RIVERO GARCIA

Cristhian Javier Cedeño Mosquera

Elberth Cecilio Rivero García

AUTORIZACIÓN DE PUBLICACIÓN

CRISTHIAN JAVIER CEDEÑO MOSQUERA, con cédula de ciudadanía 131537010-4, y ELBERTH CECILIO RIVERO GARCÍA con cédula de ciudadanía 130977350-3, autorizo a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, la publicación en la biblioteca de la institución del informe de investigación, con la modalidad proyecto de titulación, con el tema: SISTEMA DE CIBERSEGURIDAD MEDIANTE BIBLIOTECA DE CÓDIGO ABIERTO EN LOS SERVIDORES DE LOS HOSPITALES DEL IESS PROVINCIA DE MANABÍ , cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Firmado electrónicamente por:
CRISTHIAN JAVIER CEDENO MOSQUERA

Ing. Cedeño Mosquera Cristhian Javier
131537010-4

Firmado electrónicamente por:
ELBERTH CECILIO RIVERO GARCIA

Ing. Elberth Cecilio Rivero García
130977350-5

CERTIFICACIÓN DEL TUTOR

Msg. Néstor Adrián Mora, certifica haber tutelado el trabajo de titulación SISTEMA DE CIBERSEGURIDAD MEDIANTE BIBLIOTECA DE CÓDIGO ABIERTO EN LOS SERVIDORES DE LOS HOSPITALES DEL IESS PROVINCIA DE MANABÍ, que ha sido desarrollado por Ing. Cristhian Javier Cedeño Mosquera e Ing. Elberth Cecilio Rivero García, previo la obtención del título de Magíster en Ciberseguridad, de acuerdo al Reglamento de unidad de titulación de los programas de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Feliz López.

NESTOR ADRIAN MORA
MACIAS
MAESTRIA
CIBERSEGURIDAD
ESPAM MFL

Ing. Néstor Adrián Mora Macías. Mgs.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos APROBADO el trabajo de titulación SISTEMA DE CIBERSEGURIDAD MEDIANTE BIBLIOTECA DE CÓDIGO ABIERTO EN LOS SERVIDORES DE LOS HOSPITALES DEL IESS PROVINCIA DE MANABÍ, que ha sido propuesto, desarrollado y sustentado por los Ing. Cristhian Javier Cedeño Mosquera e Ing. Elberth Cecilio Rivero García, previa la obtención del título de Magíster en Ciberseguridad, de acuerdo al Reglamento de la unidad de titulación de los programa de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Firmado electrónicamente por:
DANIEL AGUSTIN MERA MARTINEZ

Mg.Sc. Daniel Agustín Mera Martínez
PRESIDENTE TRIBUNAL

Firmado digitalmente por ALFONSO TOMAS LOOR VERA

Mg.Sc. Alfonso Tomás Loor Vera
MIEMBRO TRIBUNAL

Firmado digitalmente por AURA DOLORES ZAMBRANO RENDON

Mg.Sc. Aura Dolores Zambrano Rendón
MIEMBRO TRIBUNAL

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de crecer como ser humano a través de una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día;

Al Instituto Ecuatoriano de Seguridad Social (IESS) por brindar el apoyo y la oportunidad de llevar a cabo este proyecto en los servidores de los hospitales. Su compromiso con la seguridad cibernética y la protección de la información sensible ha sido fundamental para el desarrollo de esta investigación.

A los docentes de la Escuela Superior Politécnica Manuel Félix López, quienes, con su amplio conocimiento y experiencia, me guiaron y brindaron orientación invaluable a lo largo de todo el proceso de investigación. Sus consejos y comentarios críticos fueron fundamentales para la calidad y el enriquecimiento de este trabajo.

A todas aquellas personas que, de una u otra manera, han contribuido con su apoyo, conocimientos y ánimo durante esta travesía académica. Agradezco a mis compañeros de clase, amigos y familiares por su constante apoyo, motivación y comprensión durante el desarrollo de este proyecto.

Cristhian Javier Cedeño Mosquera
Elberth Cecilio Rivero García

DEDICATORIA

A mis padres y hermanos, por estar siempre a mi lado brindándome su apoyo moral para no desmayar en las metas propuestas.

A mis hijos, por ser el soporte y fuente de inspiración y esfuerzo.

Elberth Cecilio Rivero García

DEDICATORIA

A mis amados padres y a mi querida esposa, quiero dedicarles este proyecto de titulación en ciberseguridad. Su amor, apoyo incondicional y comprensión han sido la fuerza impulsora detrás de cada paso que he dado. Gracias por creer en mí y por ser mi mayor inspiración. Este logro no habría sido posible sin su aliento constante.

Con todo mi amor y gratitud, les dedico este proyecto que representa el esfuerzo, la dedicación y el compromiso en busca de un mundo digital más seguro. ¡Gracias por ser mi mayor motivación en cada paso del camino!

Cristhian Javier Cedeño Mosquera

CONTENIDO GENERAL

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

RESUMEN

Este proyecto de titulación se enfocó en abordar la creciente preocupación por la seguridad cibernética en los hospitales del IESS en la provincia de Manabí. El objetivo principal fue implementar un sistema de ciberseguridad eficiente y efectivo utilizando una biblioteca de código abierto. Para lograrlo, se realizó un análisis exhaustivo de las vulnerabilidades y amenazas presentes en los servidores de los hospitales. Se seleccionó una biblioteca de código abierto adecuada, la cual proporcionó herramientas y funcionalidades sólidas para fortalecer la seguridad cibernética, se identificaron los riesgos potenciales en base a los resultados generados por la herramienta de análisis ejecutada. Esta biblioteca fue implementada en los servidores de los hospitales, adaptándola y configurándola para garantizar la integridad y confidencialidad de la información. Entre los resultados más relevantes se encontraron el acceso SSH a través de contraseñas vacías, Contraseña del cargador de arranque en grub2 sin configurar, Nombre de usuario administrador del cargador de arranque en un valor no predeterminado sin configurar. Las medidas correctivas aplicadas demostraron una mejora significativa en la seguridad de los servidores de los hospitales del IESS en la provincia de Manabí, reduciendo el riesgo de ataques cibernéticos, pérdida de datos y exposición de información sensible.

PALABRAS CLAVE

Sistema de Ciberseguridad, Vulnerabilidades, Integridad, Confidencialidad, Disponibilidad.

ABSTRACT

This titling project focused on addressing the growing concern about cyber security in IESS hospitals in Manabí province. The main objective was to implement an efficient and effective cybersecurity system using an open-source library. To achieve this, an exhaustive analysis of the vulnerabilities and threats present in the hospital servers was carried out. A suitable open-source library was selected, which provided robust tools and functionalities to strengthen cyber security; potential risks were identified based on the results generated by the executed analysis tool. This library was implemented in hospital servers, adapted, and configured to guarantee the integrity and confidentiality of the information. Among the most relevant results was SSH access via empty passwords, Unconfigured grub2 bootloader password, and Unconfigured bootloader admin username in a non-default value. The corrective measures applied demonstrated a significant improvement in the security of the servers of the IESS hospitals in Manabí province, reducing the risk of cyber attacks, data loss, and exposure to sensitive information.

KEYWORDS

Cybersecurity System, Vulnerabilities, Integrity, Confidentiality, Availability.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

La gestión de la ciberseguridad en las organizaciones es ahora más importante que en años anteriores, ya que la pandemia mundial ha provocado cambios importantes en el entorno informático en todos los aspectos de nuestras vidas, lo que ha generado oportunidades para que los ciberdelincuentes ataquen los sistemas, organizaciones y usuarios.

En junio de 2021, Internet Crime Complaint Center (IC3), comenzó a rastrear los incidentes de ransomware informados en los que la víctima era miembro de un sector de infraestructura crítica. Hay 16 sectores de infraestructura crítica cuyos activos, sistemas y redes, sean estos físicos o virtuales, se consideran tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en nuestra seguridad, economía nacional, salud o seguridad pública, o cualquier combinación de los mismos. destruir los datos de la víctima o divulgarlos al público.

Se realizó un estudio en América Latina que se centró en los problemas potenciales de inseguridad informática y robo de información, vulnerabilidades, piratería, phishing y otras amenazas en organizaciones financieras y de otro tipo. Según el, Ecuador ocupa el puesto 19 entre 35 países en los rankings internacionales de seguridad relacionados con la evaluación de vulnerabilidad y riesgo, con un puntaje de seguridad del 26.3%, y el puesto 74 en la pandemia de Covid-19 2020, evaluado por (Grupo de Conocimiento Profundo, 2020). En este sentido, el índice de inseguridad informática es alto, ocupando el sexto lugar entre 19 países con un índice de seguridad de 31,57%, inferior a países como Perú, Venezuela, Chile, Paraguay, El Salvador, Nicaragua y Bolivia. Unión Internacional de Telecomunicaciones (UIT) (Troein & Acayo, 2020).

Ha habido casos similares en Ecuador donde los servidores sufren de vulnerabilidades y amenazas cibernéticas. Según los datos recopilados por el Centro de Respuesta a Incidentes Informáticos (CSIRT), un equipo de respuesta responsable de detectar, prevenir y gestionar incidentes de seguridad, la tasa de

explotación de seguridad nacional es del 46,4 %, que es muy baja. En comparación con otros países, esta vulnerabilidad causada por el phishing, bots, piratería, spam y otros fenómenos externos.

La seguridad cibernética se ha convertido en un tema crítico en la gestión de la información en los hospitales del Instituto Ecuatoriano de Seguridad Social (IESS) en la provincia de Manabí. Estos hospitales almacenan información sensible de los pacientes, incluyendo su historial médico, resultados de pruebas y diagnósticos, lo que los convierte en objetivos atractivos para los ciberdelincuentes.

Aunque el IESS ha implementado medidas de seguridad informática en sus hospitales, estos sistemas pueden ser vulnerables a ataques cibernéticos cada vez más sofisticados. Por lo tanto, es necesario implementar un sistema de ciberseguridad más robusto y efectivo en los servidores de los hospitales del IESS en la provincia de Manabí para proteger la información de los pacientes y garantizar la continuidad de los servicios de atención médica.

En este contexto se plantea lo siguiente: ¿Cómo implementar un sistema de ciberseguridad mediante biblioteca de código abierto en los servidores de los hospitales del IESS provincia de Manabí que garantice la protección de la información de los pacientes y la continuidad de los servicios de atención médica?

Para resolver esta problemática que actualmente se presenta, el presente proyecto de investigación se enfoca en la implementación de un sistema de ciberseguridad mediante biblioteca de código abierto en los servidores de los hospitales del IESS en la provincia de Manabí. La investigación incluirá la revisión de la literatura existente sobre ciberseguridad y bibliotecas de código abierto, la identificación de los riesgos de seguridad en los servidores de los hospitales del IESS y la evaluación de las bibliotecas de código abierto disponibles para la implementación de un sistema de ciberseguridad.

Además, se realizará una investigación empírica para evaluar la efectividad del sistema de ciberseguridad implementado, incluyendo pruebas de penetración y evaluaciones de vulnerabilidad. La investigación también incluirá la revisión de las políticas y procedimientos de seguridad de la información existentes en los

hospitales del IESS y la recomendación de mejoras a dichas políticas y procedimientos.

1.2. JUSTIFICACIÓN

La implementación de un sistema de ciberseguridad mediante biblioteca de código abierto en los servidores de los hospitales del IESS provincia de Manabí ayudará a prevenir los riesgos de ciberataques y fugas de información confidencial. Esto puede evitar gastos adicionales en la recuperación de datos o indemnizaciones por responsabilidad civil, lo que se traduce en un ahorro significativo para la institución.

Además, se puede generar un importante ahorro económico en comparación con la adquisición de soluciones de seguridad propietarias. Las bibliotecas de código abierto se distribuyen de forma gratuita y su uso no está sujeto a licencias costosas, lo que disminuye significativamente los costos de implementación y mantenimiento.

En ese mismo contexto, la implementación de un sistema de ciberseguridad eficaz puede prevenir pérdidas económicas asociadas a ciberataques, tales como la interrupción de servicios, pérdida de datos confidenciales y prevenir estos riesgos que pueden ahorrar tiempo y recursos al Hospital.

Dentro del ámbito social la protección de la información personal de los pacientes es esencial para preservar su privacidad y dignidad, y para mantener la confianza del público en el sistema de salud.

También, en la Ley Orgánica de Protección de Datos Personales (LOPD) establece que los mismos deben ser tratados de manera legítima, transparente y respetando los derechos fundamentales de las personas. Además, se establece que los datos personales deben ser utilizados únicamente para los fines para los cuales fueron recopilados y no pueden ser divulgados a terceros sin el consentimiento explícito del titular de los datos.

Así mismo, en el Artículo 230 del COIP (CÓDIGO ÓRGÁNICO INTEGRAL PENAL) tipifica que los delitos informáticos son " todos aquellos eventos que se cometen a través del uso de tecnologías de la información y la comunicación". Estos delitos pueden incluir el acceso no autorizado a sistemas informáticos, la interceptación

ilegal de datos, el sabotaje informático, la difusión de virus o malware y otros delitos relacionados.

En relación a esto, la gestión de medidas de ciberseguridad en los hospitales es importante también dentro del marco legal, ya que actualmente es un requisito obligatorio según la normativa ecuatoriana en materia de protección de datos personales, que establece la obligación de garantizar la confidencialidad, integridad y disponibilidad de la información de los usuarios.

Finamente la implementación de un sistema de ciberseguridad mediante biblioteca de código abierto en los servidores de los hospitales del IESS provincia de Manabí es fundamental desde los aspectos económico, social, técnico y legal. Esto permitirá garantizar la confidencialidad, integridad y disponibilidad de la información, prevenir riesgos asociados a ciberataques, y mejorar la calidad de atención sanitaria y la protección de los datos personales de los pacientes.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un sistema de Ciberseguridad mediante Biblioteca de Código Abierto en los Servidores de los Hospitales del IESS Provincia de Manabí con el propósito de mitigar las vulnerabilidades encontradas.

1.3.2. OBJETIVOS ESPECÍFICOS

- Revisión bibliográfica para determinar la herramienta de análisis de vulnerabilidades a utilizar en los servidores del IESS Provincia de Manabí
- Realizar el análisis de seguridad mediante la herramienta de detección de vulnerabilidad en los servidores, con base a las políticas establecidas en el hospital del IESS.
- Implementar un sistema de seguridad mediante herramienta OpenSource en los servidores del IESS Provincia de Manabí.

- Evaluar el sistema de ciberseguridad implementado con el propósito de medir el nivel de seguridad establecido en los servidores del IESS Provincia de Manabí

1.4. IDEA A DEFENDER

¿Cómo puede la implementación de una biblioteca de código abierto mejorar la seguridad informática en los servidores de los hospitales del IESS en la provincia de Manabí?

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1. SEGURIDAD INFORMÁTICA

Según el Instituto Nacional de Ciberseguridad (INCIBE, 2021), la seguridad informática se define como "el conjunto de medidas técnicas, legales, organizativas y humanas que se aplican para proteger la información y los sistemas informáticos, asegurando su disponibilidad, confidencialidad e integridad"

La seguridad informática involucra aspectos importantes como la Integridad, Disponibilidad y Confidencialidad de la información, sin embargo; existen características que son consideradas importantes si de seguridad se habla.

La Organización Internacional de Normalización (ISO), indica que la seguridad informática se refiere a "la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un enfoque de gestión de riesgos y la implementación de controles adecuados". (ISO, 2019)

2.1.1. AMENAZAS Y RIESGOS EN ENTORNOS HOSPITALARIOS

(Benjamin, D. Kyle, Taylor, & Clemens Scott, 2019) Demostraron en su Artículo científico en el cual realizaron tres búsquedas separadas a través de las bases de datos CINAHL y PubMed (MEDLINE) y Nursing and Allied Health Source a través de ProQuest y demostraron que la industria de la salud está rezagada en seguridad. Al igual que otras industrias, la atención médica debe definir claramente los deberes de ciberseguridad, establecer procedimientos claros para actualizar el software y manejar una violación de datos, usar VLAN y desautenticación y computación basada en la nube, y capacitar a sus usuarios para que no abran códigos sospechosos.

(Avila Pesantez, Chalan Analuisa, Figueras, & Avila, 2022) Indican que, Los principales ataques a la infraestructura de red a nivel de conmutación son de suplantación de identidad, MAC-ARP (Address Resolution Protocol), ataques a Spanning Tree Protocol (STP), Vlan Hopping y Dynamic Host Configuration Protocol (DHCP) Starvation.

Del mismo modo los autores antes mencionados implementaron a nivel de red políticas de seguridad de la información en base a la detección de vulnerabilidades obteniendo los siguientes resultados:

“La implementación de las políticas propuestas y aplicadas mediante la configuración de comandos en los equipos de conmutación, demuestran los resultados de mitigación a los ataques y vulnerabilidades establecidas con un promedio de efectividad del 98% en el centro de datos hospitalario. Los ataques de overflow a la tabla CAM, ARP spoofing y MITM fueron contrarrestados en su totalidad (100%) y los restantes tienen una media del 96,5% de mitigación efectiva. El siguiente paso fue aplicar las configuraciones en los equipos físicos, concluyendo que en la infraestructura de red del centro hospitalario se aplicó los correctivos necesarios para mejorar su seguridad informática”. (Avila Pesantez, Chalan Analuisa, Figueras, & Avila, 2022)

2.1.2. SOFTWARE DE CÓDIGO ABIERTO Y SU PAPEL EN LA CIBERSEGURIDAD

El software de código abierto es aquel cuyo código fuente es accesible y puede ser utilizado, modificado y distribuido libremente por cualquier persona. En el contexto de la ciberseguridad, el software de código abierto juega un papel importante en varios aspectos. A continuación, se presenta algunas ventajas y desventajas del uso de software de código abierto en la ciberseguridad.

- **Ventajas del software de código abierto en ciberseguridad:**

Transparencia: Una de las mayores ventajas del software de código abierto en la ciberseguridad es su transparencia. Al tener acceso al código fuente, los expertos en seguridad pueden analizarlo para identificar posibles vulnerabilidades y asegurarse de que no haya puertas traseras ocultas o maliciosas. Esto permite una mayor confianza en la seguridad del software, ya que cualquier debilidad puede ser detectada y corregida por la comunidad de desarrolladores y usuarios.

Flexibilidad y personalización: El software de código abierto permite a los usuarios adaptarlo a sus necesidades específicas y personalizarlo según sus requisitos de seguridad. Esto es especialmente valioso en el ámbito de la ciberseguridad, donde

las necesidades y amenazas cambian constantemente. Los usuarios pueden modificar el código para mejorar la seguridad del software, añadir funciones de seguridad adicionales o integrarlo con otras herramientas de seguridad.

Comunidad activa: El software de código abierto suele contar con una comunidad activa de desarrolladores y usuarios que contribuyen a su mejora y seguridad. Esto significa que hay una mayor probabilidad de identificar y corregir rápidamente vulnerabilidades de seguridad. Además, al haber una comunidad activa, los usuarios pueden acceder a recursos como foros, listas de correo y documentación para obtener soporte y compartir conocimientos sobre seguridad.

Costo: El uso de software de código abierto puede ser una opción económica para la implementación de soluciones de seguridad. Al ser de libre acceso y modificación, no implica el costo de licencias de software propietario. Esto puede resultar en ahorros significativos, especialmente para organizaciones con presupuestos limitados.

- **Desventajas del software de código abierto en ciberseguridad**

Responsabilidad: Aunque la comunidad de desarrolladores y usuarios de software de código abierto es activa en la mejora y corrección de vulnerabilidades, no hay una entidad central responsable de garantizar la seguridad del software. Esto significa que los usuarios deben confiar en la comunidad y en su propia capacidad para auditar y mantener la seguridad del software.

Falta de soporte: A diferencia del software propietario, que a menudo viene con soporte técnico y actualizaciones regulares, el software de código abierto puede carecer de un soporte formal. Esto puede representar un desafío para las organizaciones que necesitan un nivel alto de soporte y garantías en términos de seguridad.

Fragmentación y compatibilidad: La naturaleza abierta y descentralizada del software de código abierto puede resultar en una mayor fragmentación y diversidad de versiones y distribuciones. Esto puede dificultar la compatibilidad y la estandarización en un entorno de seguridad, lo que requiere un mayor esfuerzo de integración y gestión.

2.2. CIBERSEGURIDAD

(Cornejo Montoya, Verdezoto, & Villacís, 2019), Conjunto de acciones que persigue la protección de la información de las organizaciones y en general de toda la comunidad que está en el ciberespacio.

(ORGANIZACIÓN INTERNACIONAL DE COMISIONES DE VALORES, 2020). "Más allá de la protección operativa de los sistemas y redes, la ciberseguridad es, y seguirá siendo, fundamental para garantizar la integridad y la capacidad de recuperación de los procesos socioeconómicos interconectados, de gobierno y de negocios que operan en el marco del siempre complejo ecosistema tecnológico, por lo que aborda el riesgo cibernético en todos los ámbitos. requiere continuos esfuerzos y adaptación.

2.2.1. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES OPENSOURCE

El análisis de vulnerabilidades es el conjunto de pruebas de seguridad, en donde un especialista ejecuta técnicas y herramientas especializadas para la detección de fallas o malas configuraciones y vulnerabilidades asociadas a los servicios y activos de TI de una organización. (Marcillo Parrales, 2021)

Existe actualmente varias herramientas de análisis de vulnerabilidades de código abierto disponibles para su uso en la seguridad informática. A continuación, se presentan algunas de las herramientas más usadas:

a) **OpenVAS**: Es una plataforma de escaneo de vulnerabilidades de código abierto que se utiliza para identificar vulnerabilidades en redes y sistemas. Proporciona una amplia gama de pruebas de seguridad y análisis de vulnerabilidades.
b) **Nmap**: Es una herramienta de escaneo de redes y sistemas de código abierto que se utiliza para identificar los dispositivos conectados a una red, sus sistemas operativos y los servicios en ejecución. También puede utilizarse para identificar posibles vulnerabilidades en la red.
c) **Metasploit**: Es un marco de prueba de penetración y explotación de código abierto que se utiliza para evaluar la seguridad de sistemas y aplicaciones

informáticas. Permite a los usuarios probar la seguridad de sistemas y aplicaciones mediante la simulación de ataques de seguridad.

d) **Wireshark**: Es una herramienta de análisis de tráfico de red de código abierto que se utiliza para capturar y analizar paquetes de datos en una red. Puede utilizarse para identificar posibles vulnerabilidades en el tráfico de red y ayudar a mejorar la seguridad de la red.
e) **Nikto**: Es una herramienta de escaneo de vulnerabilidades web de código abierto que se utiliza para identificar posibles vulnerabilidades en servidores web. Puede utilizarse para realizar pruebas de seguridad en sitios web y aplicaciones web para identificar posibles vulnerabilidades y mejorar su seguridad.
f) **OSSEC**: Es un sistema de detección de intrusiones de código abierto que se utiliza para monitorear la seguridad de los sistemas y las redes. Proporciona alertas y notificaciones en tiempo real cuando se detectan posibles amenazas de seguridad.

2.2.2. ESTANDARES DE SEGURIDAD INFORMÁTICA

Los estándares de seguridad informática son normas y pautas que establecen las mejores prácticas y requisitos para asegurar la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos. Estos estándares son desarrollados y publicados por diversas organizaciones y entidades, y su cumplimiento puede ser requerido por regulaciones, leyes o políticas internas de una organización. Algunos de los estándares de seguridad informática más ampliamente utilizados son:

- **ISO/IEC 27001**: Esta norma establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Proporciona un enfoque basado en el riesgo para identificar, evaluar y gestionar los riesgos de seguridad de la información, y establece controles y procesos para garantizar la seguridad de la información en una organización.

- **NIST SP 800-53**: Este es un conjunto de controles de seguridad desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos para sistemas federales de información. Es ampliamente

utilizado en el gobierno de Estados Unidos y en muchas organizaciones del sector privado como marco de referencia para asegurar la información y los sistemas.

- **CIS Controls**: Los Controles de Seguridad Críticos del Centro de Internet Segura (CIS) son un conjunto de mejores prácticas de seguridad informática que ofrecen una lista prioritizada de acciones concretas y eficaces para mejorar la seguridad de la información en una organización. Son ampliamente utilizados como guía para implementar medidas de seguridad.

2.2.3. NORMATIVAS Y REGULACIONES RELEVANTES PARA LA PROTECCIÓN DE SISTEMAS INFORMÁTICAS

En el sector de la salud, la protección de sistemas informáticos es de vital importancia para salvaguardar la confidencialidad, integridad y disponibilidad de la información médica sensible. Existen varias normativas y regulaciones relevantes a nivel internacional y regional que establecen requisitos específicos para la protección de sistemas informáticos en el sector de la salud. Algunas de las normativas y regulaciones más importantes son:

- Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) en Estados Unidos: HIPAA es una regulación federal que establece estándares para la privacidad, seguridad y notificación de violaciones de datos de información de salud protegida (PHI, por sus siglas en inglés) en Estados Unidos. HIPAA establece requisitos para la protección de sistemas informáticos en organizaciones cubiertas, como hospitales, clínicas y proveedores de atención médica, incluyendo la implementación de medidas de seguridad técnicas y administrativas.

- Reglamento General de Protección de Datos (GDPR) en la Unión Europea: El GDPR es una regulación de la Unión Europea que establece requisitos para la protección de datos personales, incluyendo datos de salud, en toda la UE. El GDPR establece medidas de seguridad técnicas y organizativas que deben ser implementadas en sistemas informáticos de organizaciones

que procesan datos personales de ciudadanos de la UE, incluyendo organizaciones de atención médica.

- Ley de Tecnologías de la Información y Comunicación para el Sector Salud (Ley TICSS) en México: La Ley TICSS es una regulación en México que establece requisitos para la seguridad y protección de la información de salud en sistemas informáticos en el sector de la salud. Esta ley establece medidas de seguridad técnicas y organizativas que deben ser implementadas en sistemas informáticos de organizaciones de atención médica en México.

- Ley de Protección de Datos Personales en Salud (LPDPS) en Argentina: La LPDPS es una regulación en Argentina que establece requisitos para la protección de datos personales en el sector de la salud. Esta ley establece medidas de seguridad técnicas y organizativas que deben ser implementadas en sistemas informáticos de organizaciones de atención médica en Argentina.

2.3. GESTIÓN DE RIESGOS EN SEGURIDAD INFORMÁTICA

La gestión de riesgos en seguridad informática es un proceso continuo que tiene como objetivo identificar, evaluar, controlar y mitigar los riesgos asociados a la seguridad de la información en una organización. La gestión de riesgos en seguridad informática es fundamental para proteger los sistemas informáticos y la información confidencial de la organización.

A continuación, se presentan los pasos esenciales para llevar a cabo la gestión de riesgos en seguridad informática:

Identificación de los activos de información: Es importante identificar los activos de información críticos de la organización, incluyendo los sistemas informáticos, la información confidencial y los recursos humanos.

Evaluación de los riesgos: Una vez que se han identificado los activos de información, es necesario evaluar los riesgos asociados a cada uno de ellos, teniendo en cuenta las posibles amenazas y vulnerabilidades.

Análisis de los riesgos: Una vez que se han evaluado los riesgos, es necesario analizarlos para determinar la probabilidad de que ocurran y el impacto que tendrían en la organización.

Evaluación de la efectividad de los controles existentes: Es importante evaluar los controles de seguridad existentes en la organización y determinar si son efectivos para mitigar los riesgos identificados.

Identificación de nuevas medidas de control: Si se determina que los controles existentes no son suficientes para mitigar los riesgos, es necesario identificar nuevas medidas de control que puedan implementarse para proteger los activos de información.

Implementación de medidas de control: Una vez que se han identificado las nuevas medidas de control, es necesario implementarlas y asegurarse de que sean efectivas para mitigar los riesgos identificados.

Monitoreo y revisión continua: Es importante monitorear y revisar continuamente los riesgos y las medidas de control implementadas para asegurarse de que sigan siendo efectivas a lo largo del tiempo.

2.3.1. ANÁLISIS Y EVALUACIÓN DE RIESGOS EN ENTORNOS HOSPITALARIOS

La seguridad en entornos hospitalarios es un tema crítico, ya que se maneja una gran cantidad de información sensible y confidencial. Por esta razón, es importante llevar a cabo un análisis y evaluación de riesgos para garantizar la protección de la información y la continuidad de los servicios. A continuación, se presentan algunas consideraciones a tener en cuenta para el análisis y evaluación de riesgos en entornos hospitalarios:

Identificación de activos críticos: En primer lugar, es necesario identificar los activos críticos, como los sistemas de información, dispositivos médicos y bases de datos, que son esenciales para la prestación de servicios médicos. Debe establecerse una jerarquía de importancia de los activos para enfocar la evaluación de riesgos en los activos más críticos.

Identificación de amenazas: Se debe identificar las posibles amenazas a los activos críticos, como ataques informáticos, malware, robo de datos y desastres naturales. Las amenazas deben clasificarse en función de su probabilidad de ocurrencia y su impacto en los activos.

Evaluación de vulnerabilidades: Una vez identificadas las amenazas, se debe evaluar las vulnerabilidades de los activos críticos que pueden ser explotadas por los atacantes. Las vulnerabilidades pueden ser técnicas, como las debilidades de seguridad en los sistemas de información, o humanas, como el uso de contraseñas débiles o la falta de capacitación de los empleados.

Análisis de riesgos: Con la información recopilada, se debe realizar un análisis de riesgos para identificar los riesgos críticos, sus probabilidades de ocurrencia y los impactos potenciales. La evaluación de riesgos debe ser una evaluación cuantitativa y cualitativa, en la que se puedan comparar los riesgos identificados.

Mitigación de riesgos: Una vez identificados los riesgos, se deben tomar medidas para mitigarlos. Esto puede incluir la implementación de medidas de seguridad, como firewalls, sistemas de detección de intrusiones, políticas de seguridad de contraseñas, respaldo de datos, entre otros. También es importante capacitar a los empleados sobre las mejores prácticas de seguridad y realizar pruebas regulares de penetración para identificar debilidades en la seguridad.

Finalmente, el análisis y evaluación de riesgos en entornos hospitalarios es un proceso crítico para garantizar la protección de la información y la continuidad de los servicios médicos. La identificación de activos críticos, amenazas, vulnerabilidades y el análisis de riesgos deben ser una parte integral de la gestión de seguridad en estos entornos.

2.4. ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

El análisis de vulnerabilidades y las pruebas de penetración son dos técnicas de seguridad informática que se utilizan para identificar debilidades en los sistemas de información y evaluar su capacidad para resistir ataques externos. A continuación, se presentan algunas consideraciones a tener en cuenta para el análisis de vulnerabilidades y las pruebas de penetración.

2.4.1. ANÁLISIS DE VULNERABILIDADES

Identificación de los activos a analizar: En primer lugar, es necesario identificar los sistemas de información, dispositivos y aplicaciones que se analizarán.

Selección de herramientas de análisis: Existen numerosas herramientas de análisis de vulnerabilidades disponibles en el mercado, tanto gratuitas como comerciales. Es importante seleccionar una herramienta que se ajuste a las necesidades de la organización y que permita identificar la mayor cantidad de vulnerabilidades posible.

Escaneo de vulnerabilidades: Una vez seleccionada la herramienta, se debe realizar un escaneo de vulnerabilidades para identificar debilidades en los sistemas y aplicaciones.

Evaluación de resultados: Una vez finalizado el escaneo, se deben revisar los resultados y evaluar el impacto de las vulnerabilidades identificadas. Es importante priorizar las vulnerabilidades en función de su gravedad y el riesgo que representan para la organización.

2.4.2. PRUEBAS DE PENETRACIÓN

Definición del alcance: Antes de realizar una prueba de penetración, es necesario definir el alcance de la prueba y los sistemas y aplicaciones que se van a evaluar.

Selección de un equipo de pruebas: Las pruebas de penetración deben ser realizadas por profesionales de seguridad informática experimentados y capacitados para realizar pruebas de forma segura.

Identificación de posibles impactos: Antes de realizar la prueba, es necesario identificar posibles impactos en los sistemas y aplicaciones. Esto puede incluir la pérdida de datos o el tiempo de inactividad.

Ejecución de la prueba: Una vez que se han tomado todas las medidas necesarias para realizar la prueba de forma segura, se debe ejecutar la prueba y registrar los resultados.

Evaluación de resultados: Después de la prueba, se deben evaluar los resultados y determinar la gravedad de las vulnerabilidades identificadas. Es importante priorizar las vulnerabilidades en función de su gravedad y el riesgo que representan para la organización.

Es así que, tanto el análisis de vulnerabilidades como las pruebas de penetración son técnicas importantes para evaluar la seguridad de los sistemas de información y prote8ger la información de la organización. Es importante llevar a cabo estas actividades de forma regular para identificar y corregir debilidades en los sistemas antes de que sean explotadas por atacantes externos.

2.5. METODOLOGÍAS, TÉCNICAS Y HERRAMIENTAS

Existen varias metodologías, técnicas y herramientas que se pueden utilizar para la gestión de la seguridad informática en una organización. A continuación, se presentan algunas de las más comunes.

2.5.1. METODOLOGÍAS

ISO 27001: Esta es una norma internacional que establece un marco de referencia para la gestión de la seguridad de la información. La norma ISO 27001 incluye un conjunto de controles que pueden ayudar a una organización a proteger sus sistemas de información.

NIST: El National Institute of Standards and Technology (NIST) es una organización gubernamental de Estados Unidos que establece estándares para la gestión de la seguridad informática. El NIST Framework for Improving Critical Infrastructure Cybersecurity es una guía que las organizaciones pueden utilizar para mejorar su seguridad informática.

COBIT: Control Objectives for Information and Related Technology (COBIT) es una guía de buenas prácticas para la gestión de la seguridad de la información. COBIT se enfoca en el control y la gestión de los procesos de TI y se utiliza para asegurar que las políticas y los controles de seguridad estén en su lugar.

2.5.2. TÉCNICAS

Análisis de riesgos: El análisis de riesgos es una técnica que se utiliza para identificar y evaluar las amenazas a la seguridad de la información y los riesgos asociados con ellas. El objetivo es identificar las vulnerabilidades y los riesgos de seguridad en los sistemas de información y evaluar su impacto en la organización.

Pruebas de penetración: Las pruebas de penetración son una técnica que se utiliza para evaluar la seguridad de los sistemas de información. El objetivo es simular un ataque externo para identificar y corregir las vulnerabilidades en los sistemas antes de que sean explotadas por atacantes reales.

Monitoreo de la seguridad: El monitoreo de la seguridad es una técnica que se utiliza para detectar y responder a los eventos de seguridad en tiempo real. Esto incluye la supervisión de los registros de auditoría, la detección de actividad inusual y la evaluación de los informes de incidentes de seguridad.

2.5.3. HERRAMIENTAS

Firewalls: Los firewalls son una herramienta de seguridad informática que se utiliza para proteger los sistemas de información contra el acceso no autorizado. Los firewalls pueden configurarse para bloquear el tráfico no deseado y permitir solo el acceso a los servicios necesarios.

Antivirus: El software antivirus es una herramienta que se utiliza para detectar y eliminar malware en los sistemas de información. Los programas antivirus pueden

configurarse para escanear automáticamente los sistemas y detectar y eliminar cualquier software malicioso.

Sistemas de detección de intrusiones: Los sistemas de detección de intrusiones (IDS) son herramientas que se utilizan para monitorear los sistemas de información en busca de actividad maliciosa. Los IDS pueden alertar al personal de seguridad sobre posibles amenazas de seguridad.

CAPÍTULO III. DESARROLLO METODOLÓGICO

3.1. Revisión Bibliográfica para determinar la herramienta de escaneo de vulnerabilidades

- **Búsqueda de información** Se van a utilizar las bases de datos especializadas en el campo de la ciberseguridad, como IEEE Xplore, ACM Digital Library, así mismo la red de revistas científicas Redalyc y el motor de búsqueda Google Académico.
- **Selección de la información relevante**: Se seleccionará la información que tenga similitud del tema del proyecto y de esta manera discernir la información más relevante.
- **Evaluación de las herramientas de análisis de vulnerabilidades de ciberseguridad**: Se comparará las herramientas de análisis de vulnerabilidades de ciberseguridad identificadas y seleccionar la herramienta que mejor se adapte a los objetivos y necesidades del proyecto de investigación.
- **Informe final**. Finalmente, se elaborará una matriz detallada de la revisión bibliográfica realizada, la evaluación de las herramientas de análisis de vulnerabilidades de ciberseguridad y la conclusión de la herramienta de análisis de vulnerabilidades a utilizar

3.2. Instalación, Configuración y Ejecución de la herramienta de escaneo de vulnerabilidades

- **Configuración de OpenSCAP**: Una vez que se han definido los objetivos del análisis, configuraremos la herramienta OpenSCAP con los perfiles correspondientes y de esta manera establecer las políticas de escaneo.

- **Ejecutar un escaneo completo**: Una vez que se ha realizado el escaneo inicial, se puede ejecutar un escaneo completo utilizando los perfiles de seguridad previamente configurados. Esto ayudará a identificar cualquier vulnerabilidad que exista en el sistema.

- **Analizar los resultados del escaneo**: Mediante las plantillas de informes detallados de OpenSCAP se realizará una evaluación de los riesgos encontrados ya que nos permitirá identificar los nudos críticos a nivel de Seguridad

- **Mitigar las vulnerabilidades identificadas**: En base al informe de vulnerabilidades proporcionado por la herramienta se implementará las medidas de seguridad necesarias para mitigar los riegos encontrados.

3.3. Evaluación de las correcciones aplicadas para determinar el nivel de seguridad conseguido

- **Establecimiento de criterios de evaluación.** Se definirán los criterios y métricas que se utilizarán para evaluar el nivel de seguridad conseguido. Entre estos criterios de evaluación se encuentra la ausencia de vulnerabilidades críticas, el cumplimiento de estándares de seguridad específicos y el porcentaje de vulnerabilidades corregidas

3.4. UBICACIÓN

Tabla 1. Ubicación de Servidores de los Hospitales del IESS Provincia de Manabí

Provincia	Cantón	Ubicación	Sistema Operativo	Versión
Manabí	Chone	Rack Principal	CentOS 7	Reléase 7.9.2009 (core)
Manabí	Portoviejo	Rack Principal	CentOS 7	Reléase 7.9.2009 (core)
Manabí	Manta	Rack Principal	CentOS 7	Reléase 7.9.2009 (core)

3.5. TIPO Y ENFOQUE DE LA INVESTIGACIÓN

El enfoque de esta investigación se centra en el desarrollo de un sistema de ciberseguridad mediante el uso de una biblioteca de código abierto, específicamente OpenSCAP, en los servidores de los hospitales del IESS en la

provincia de Manabí. El objetivo principal es mejorar la seguridad de la infraestructura tecnológica de estos hospitales, protegiendo la confidencialidad, integridad y disponibilidad de la información crítica relacionada con la atención médica y los datos de los pacientes.

La creciente dependencia de los sistemas informáticos en los hospitales ha aumentado la necesidad de implementar medidas sólidas de ciberseguridad para mitigar los riesgos asociados con las amenazas cibernéticas. Mediante la utilización de la biblioteca de código abierto OpenSCAP, se busca realizar un análisis exhaustivo de los servidores, identificando vulnerabilidades y configuraciones inseguras que puedan comprometer la seguridad de los sistemas de información.

Este enfoque de investigación combinará la revisión bibliográfica especializada en el ámbito de la ciberseguridad en el sector de la salud. Se buscará adaptar y personalizar los perfiles de seguridad proporcionados por OpenSCAP a los requisitos y características específicas de los servidores de los hospitales del IESS en Manabí, y se realizarán pruebas exhaustivas para evaluar su efectividad.

El resultado de esta investigación proporcionará recomendaciones y acciones correctivas específicas para fortalecer la ciberseguridad de los servidores de los hospitales, promoviendo un entorno tecnológico más seguro y confiable. Además, se espera que los hallazgos y la metodología desarrollada puedan ser aplicados en otros hospitales y organizaciones de salud, contribuyendo así a la protección de la información sensible y a la preservación de la calidad de la atención médica.

3.6. MÉTODO DE LA INVESTIGACIÓN

En el contexto de la revisión bibliográfica para determinar la herramienta adecuada para el análisis de vulnerabilidades en servidores, es fundamental contar con información actualizada y precisa relacionada con la seguridad informática. Para ello, se llevó a cabo una búsqueda exhaustiva y selectiva para identificar bases de datos especializadas en ciberseguridad. Estas bases de datos son fuentes de información confiables y actualizadas que almacenan contenido relevante y específico sobre vulnerabilidades, herramientas de seguridad, investigaciones y

mejores prácticas en el campo de la ciberseguridad, las bases de datos a utilizar en este proyecto son IEEE Xplore y ACM Digital Library.

Mediante el uso de técnicas de búsqueda avanzada y criterios de selección específicos, se llevaron a cabo consultas en las bases de datos para extraer información relevante en relación con el objetivo de encontrar la herramienta adecuada para el análisis de vulnerabilidades en servidores.

Palabra clave utilizada = vulnerability analysis using an open source tool

Base de datos = IEEE XPLORE

Resultados Obtenidos = 82 artículos

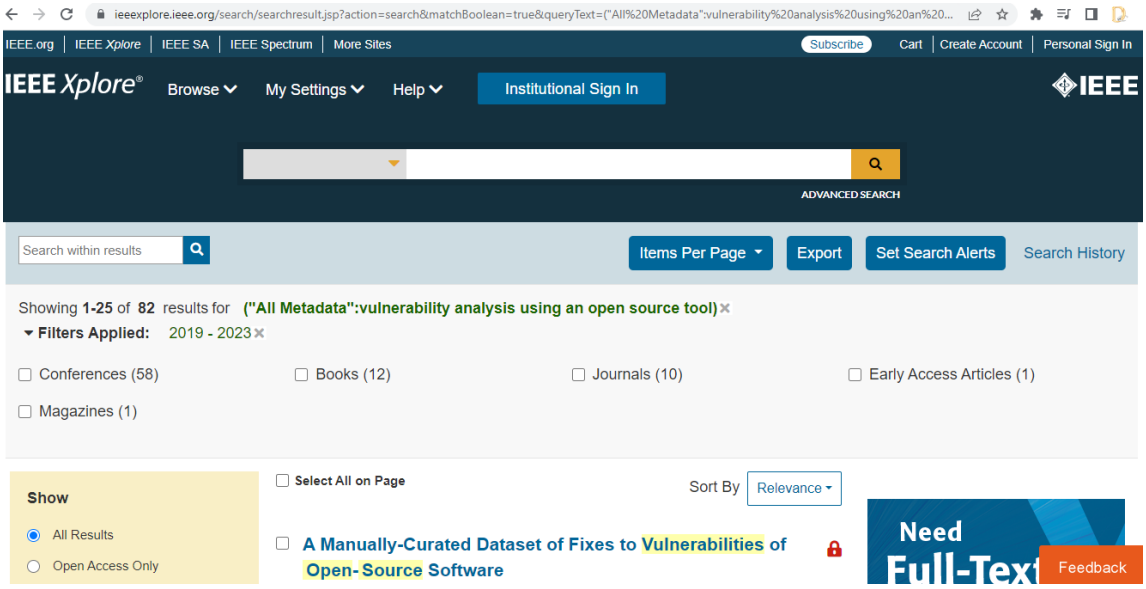


Ilustración 1. Resultados de base de datos IEEE XPLORE

Palabra clave utilizada = vulnerability analysis using an open source tool

Base de datos = ACM Digital Library

Resultados = 177.888

Ilustración 2. Resultados de base de datos ACM Digital Library

Una vez obtenida la información de las bases de datos especializadas, se procedió a evaluar y analizar la relevancia y calidad de los recursos encontrados. Se tuvieron en cuenta factores como la reputación de las fuentes, la actualidad de la información, la validez de los estudios y la coherencia de los hallazgos con el objetivo de determinar la herramienta adecuada para el análisis de vulnerabilidades en servidores.

Tabla 2. Estudio comparativo con trabajo relacionado

Campo de estudio	Periodo de publicación	Objetivo	Resultados
Infraestructura de red	2018	Diseñar una metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali-Linux	La herramienta Nmap, Wireshark y Nessus ayudó a encontrar de manera satisfactoria vulnerabilidades críticas, altas y moderadas en servidores que conforman redes de datos

Pymes	2020	Realizar una estrategia ciberseguridad de código abierto utilizando pautas de implementación técnica de seguridad (STIG)	Las herramientas OpenScap Z ofrecen un escaneo exhaustivo de vulnerabilidades en servidores, mientras que la herramienta ElasticSearch y Kibana se destaca la tener la capacidad de visualizar y explorar datos que se encuentran indexados
Infraestructura de red	2018	Herramienta personalizada, NetSecuritas, que implementa un novedoso algoritmo de generación de gráficos de ataque basado en heurística e integra diferentes fases de evaluación de la seguridad de la red.	El uso de la herramienta NetSecuritas redujo significativamente el número de vulnerabilidades críticas en la Infraestructura de red

La utilización de bases de datos especializadas en ciberseguridad permitió recopilar una variedad de recursos de calidad y actualizados en relación con el análisis de vulnerabilidades en servidores. Esta revisión bibliográfica rigurosa y basada en fuentes confiables ha proporcionado los fundamentos necesarios para tomar decisiones informadas en la selección de la herramienta adecuada, basada en la evidencia y las mejores prácticas identificadas en la literatura especializada.

Tabla 3. *Herramientas de análisis de vulnerabilidades y sus características*

Herramienta	**Enfoque**	**Modos de Escaneo**	**Personalización**	**Interfaz de Usuario**
OpenSCAP, (Red Hat, 2023)	Windows, Linux.	Normas de seguridad, NIST, etc.	Pruebas estandarizadas basadas en normas de seguridad.	Flexible
Ecsypno SCNR, (Laskos, 2023)	Se centra en el escaneo de aplicaciones web	Escaneo de pruebas de penetración	Ecsypno SCNR permite a los usuarios personalizar los escaneos y las	Interfaz de usuario más avanzada

			pruebas que se deben realizar	
OpenVAS, (Greenbone Networks, 2023)	Sistemas y aplicaciones, incluyendo vulnerabilidades de software, configuraciones inseguras y otros problemas de seguridad	Escaneo completo, un escaneo de objetivos específicos y un escaneo de recursos específicos	Está disponible a través de la creación de perfiles de escaneo y la edición de la configuración avanzada	Es una combinación de línea de comandos y gráfica
Wapiti, (Surribas, 2023)	Análisis de vulnerabilidades en aplicaciones web, incluyendo inyecciones SQL, XSS, LFI, RFI	Modo de escaneo completo, modo de escaneo incremental y modo de escaneo de URL	Está disponible a través de la creación de perfiles de escaneo y la edición de la configuración avanzada	La interfaz de usuario es en línea de comandos
Vega, (Subgraph, 2023)	Se enfoca en encontrar vulnerabilidades en aplicaciones web	Proporciona varios modos de escaneo para adaptarse a sus necesidades	Disponible a través de scripts y configuraciones avanzadas	Fácil de usar con una buena organización de la información.

Después de analizar las características de las diferentes herramientas de código abierto para el análisis de vulnerabilidades, se concluye que OpenSCAP es la opción óptima para el proyecto. A continuación, se resumen las razones:

- Amplio soporte de estándares: OpenSCAP es compatible con una variedad de estándares reconocidos, como los del NIST, lo que garantiza una evaluación integral de la seguridad y el cumplimiento normativo.
- Generación de informes detallados: OpenSCAP proporciona informes exhaustivos y comprensibles que resumen los resultados de las

evaluaciones de seguridad, lo que facilita la identificación de vulnerabilidades y la toma de acciones correctivas.

- Adaptabilidad a diferentes entornos: OpenSCAP puede adaptarse a diferentes entornos tecnológicos, lo que lo hace adecuado para evaluar la seguridad de los servidores de los hospitales del IESS en la provincia de Manabí.

- Evaluación de configuraciones y escaneo de vulnerabilidades: OpenSCAP ofrece un conjunto completo de funcionalidades, permitiendo evaluar tanto las configuraciones de los servidores como las vulnerabilidades conocidas.

En resumen, OpenSCAP destaca por su amplio soporte de estándares, generación de informes detallados, adaptabilidad y capacidad para realizar evaluaciones de configuraciones y escaneo de vulnerabilidades. Estas características hacen de OpenSCAP la opción más óptima para llevar a cabo el análisis de vulnerabilidades en los servidores de los hospitales del IESS en la provincia de Manabí.

3.7. TÉCNICAS DE INVESTIGACIÓN

3.7.1. Preparación del entorno

Antes de comenzar el escaneo de vulnerabilidades, se debe preparar el entorno de trabajo. Esto implica instalar y configurar OpenSCAP en el sistema desde el cual se realizará el escaneo. También es necesario asegurarse de que OpenSCAP tenga acceso a los servidores que se van a analizar, ya sea a través de la red o mediante la instalación de agentes en los servidores.

3.7.2. Selección de perfiles de seguridad

OpenSCAP proporciona diferentes perfiles de seguridad predefinidos que se pueden utilizar para escanear los servidores en busca de vulnerabilidades. Estos perfiles están basados en estándares de seguridad reconocidos, como el SCAP (Security Content Automation Protocol). En este paso, se selecciona el perfil de seguridad adecuado que mejor se ajuste a los requisitos y características de los servidores de los hospitales del IESS en la provincia de Manabí.

3.7.3. Ejecución del escaneo

Una vez que se han seleccionado los perfiles de seguridad, se procede a ejecutar el escaneo utilizando OpenSCAP. Durante este proceso, OpenSCAP examinará los servidores en busca de vulnerabilidades conocidas, siguiendo las pautas establecidas por el perfil de seguridad seleccionado. Utilizará una variedad de técnicas, como el análisis de configuraciones, la verificación de la presencia de parches de seguridad, y la identificación de configuraciones inseguras o incorrectas.

3.7.4. Análisis de resultados

Después de que el escaneo se haya completado, OpenSCAP generará un informe detallado con los resultados del análisis. El informe mostrará las vulnerabilidades encontradas, junto con información relevante, como la descripción de la vulnerabilidad, su gravedad y las recomendaciones para solucionarla. Este informe permitirá comprender el estado de seguridad de los servidores y priorizar las acciones correctivas.

3.7.5. Acciones correctivas

Una vez que se hayan identificado las vulnerabilidades, se deben tomar las medidas necesarias para corregirlas y fortalecer la seguridad de los servidores. Esto puede implicar aplicar parches de seguridad, modificar configuraciones, actualizar software o implementar soluciones adicionales de seguridad, según sea necesario. Es importante llevar un registro de las acciones correctivas tomadas para garantizar que se aborden adecuadamente todas las vulnerabilidades identificadas.

3.8. HERRAMIENTAS

OpenSCAP se ha seleccionado como la herramienta principal en esta investigación para evaluar la seguridad de los servidores de los hospitales del IESS en la provincia de Manabí. OpenSCAP es una biblioteca de código abierto que ofrece un conjunto de herramientas y estándares ampliamente reconocidos en el ámbito de la seguridad de la información.

Una de las ventajas clave de OpenSCAP es su capacidad para realizar análisis detallados y exhaustivos de la configuración de los servidores, identificando vulnerabilidades y riesgos potenciales. Utilizando perfiles de seguridad predefinidos y personalizados, OpenSCAP permite escanear y evaluar tanto la infraestructura física como la configuración del software de los servidores.

Es compatible con una amplia variedad de plataformas y sistemas operativos, lo que lo convierte en una herramienta flexible y adaptable para evaluar la seguridad de los servidores en diferentes entornos hospitalarios. Su enfoque basado en estándares, como los del National Institute of Standards and Technology (NIST), proporciona una base sólida para realizar análisis de cumplimiento normativo y aplicar las mejores prácticas de seguridad.

Además, OpenSCAP permite generar informes detallados sobre los resultados de las evaluaciones de seguridad, lo que facilita la identificación y priorización de las vulnerabilidades encontradas. Estos informes pueden ser utilizados como base para desarrollar estrategias de mitigación y acciones correctivas efectivas, mejorando así la postura de seguridad general de los servidores.

Al utilizar OpenSCAP como herramienta principal, se garantiza un enfoque riguroso y confiable en la evaluación de la seguridad de los servidores en los hospitales del IESS en Manabí. La capacidad de OpenSCAP para identificar y abordar vulnerabilidades específicas y personalizadas en los servidores es fundamental para fortalecer la ciberseguridad y proteger la integridad de la información crítica en el entorno hospitalario.

3.9. PROCEDIMIENTOS DE LA INVESTIGACIÓN

En esta etapa del proyecto se elaboró el procedimiento que se llevó a cabo para cumplir con los últimos objetivos planteados como son la ejecución de una herramienta de escaneo de vulnerabilidades análisis de resultados obtenidos y configuración de los servidores para corregir las vulnerabilidades encontradas.

3.9.1. Instalación, Configuración y Escaneo de Vulnerabilidades

Instalación de OpenSCAP en los servidores del Hospital Básico Chone.

Los pasos que se implementaron para la instalación y configuración de OpenSCAP en el servidor del Hospital Básico Chone, Hospital General Manta y Hospital General Portoviejo son básicamente iguales por lo que a continuación se detalla paso a paso el proceso realizado para la instalación y escaneo de vulnerabilidades en el Hospital Básico Chone.

- Ejecución en una terminal el siguiente comando: sudo yum install openscap scap-security-guide -y

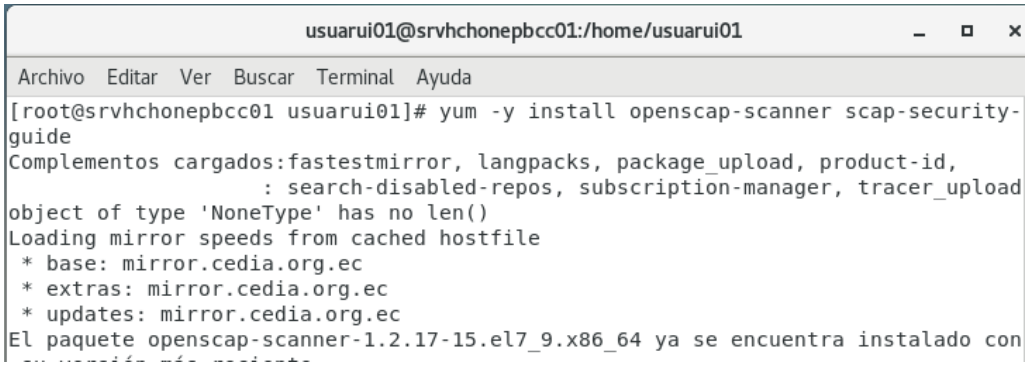


Ilustración 3. Instalación de OpenSCAP en Servidor del Hospital Básico Chone

- Revisión de los perfiles existentes de OpenSCAP mediante el siguiente comando: Oscap info /usr/share/xml/scap/ssg/content/ssg/centos7-ds.xml

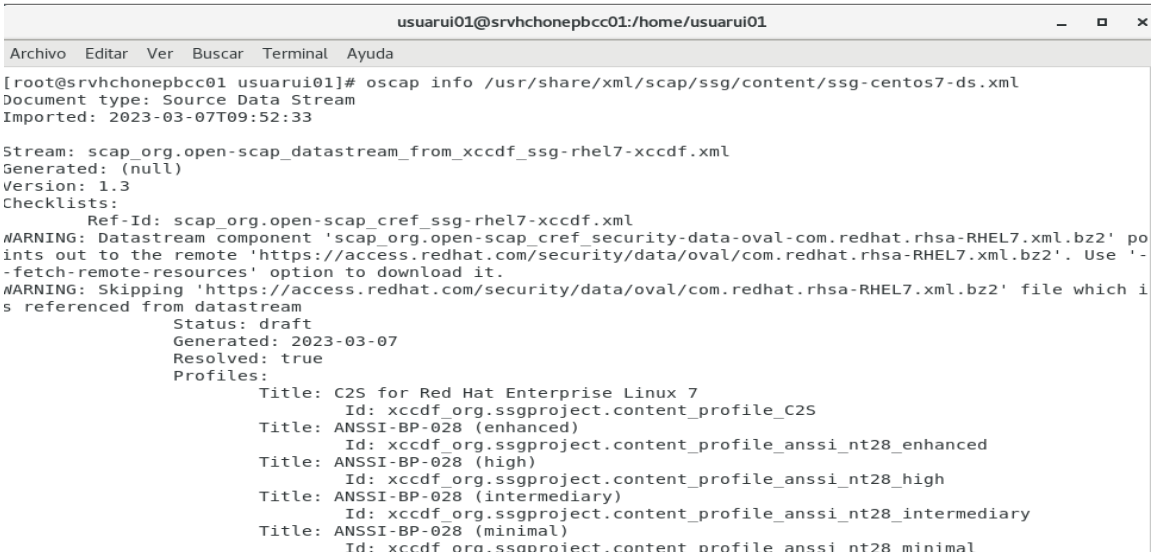


Ilustración 4. *Perfiles existentes de OpenSCAP para el escaneo de vulnerabilidades en el Servidor del Hospital Básico Chone*

- Escaneo de vulnerabilidades

El perfil que se utilizó para el escaneo de vulnerabilidades es: xccdf_org.ssgprojetct.content_profile_stig_gui, este perfil nos permite realizar un escaneo completo del servidor. El comando que se ejecuto es el siguiente:

sudo Oscap xccdf eval –profile xccdf_org.ssgprojetct.content_profile_stig_gui --report /tmp/ReporteChone.html /usr/share/xml/scap/ssg/content/ssg-centos7-ds.xml

Teniendo en cuenta que después de –report se debe de especificar la dirección donde se desea que se guarde el reporte final para que de esta manera poder analizar los resultados generados mediante un navegador web.

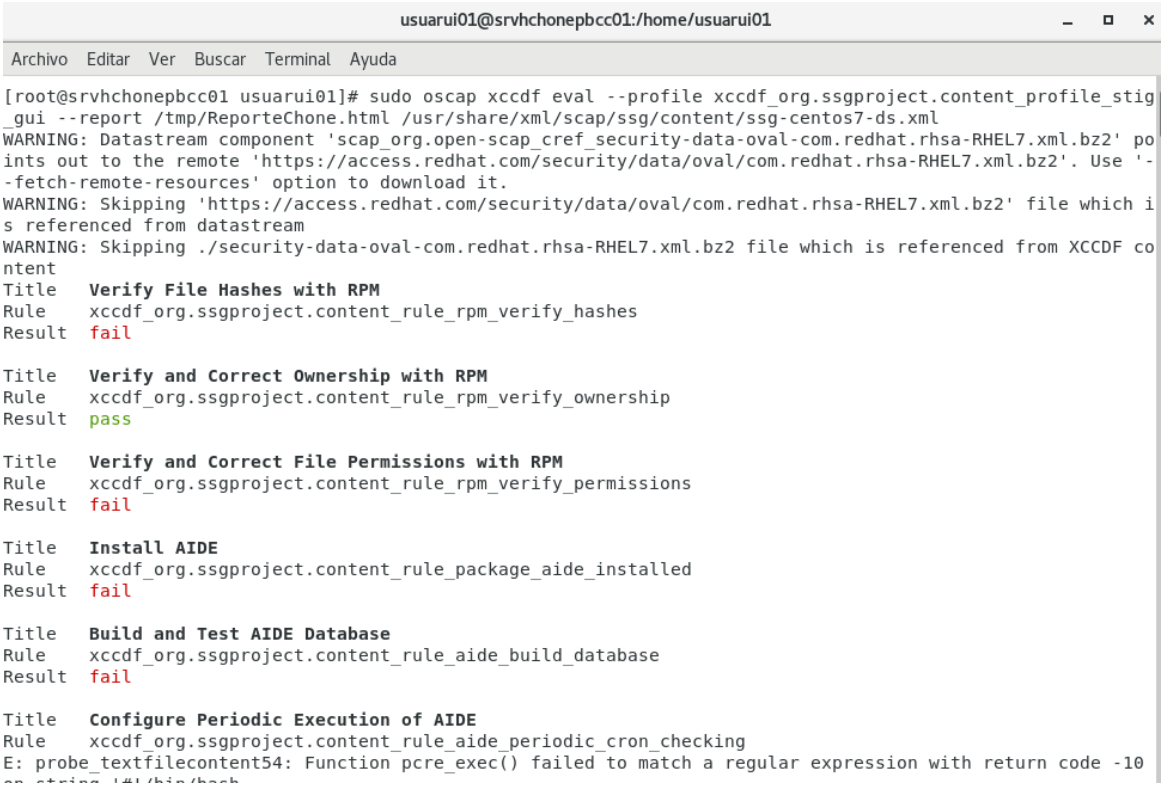


***Ilustración 5**. Escaneo de vulnerabilidades en los servidores del Hospital Básico Chone*

Instalación de OpenSCAP en los servidores del Hospital General de Portoviejo.

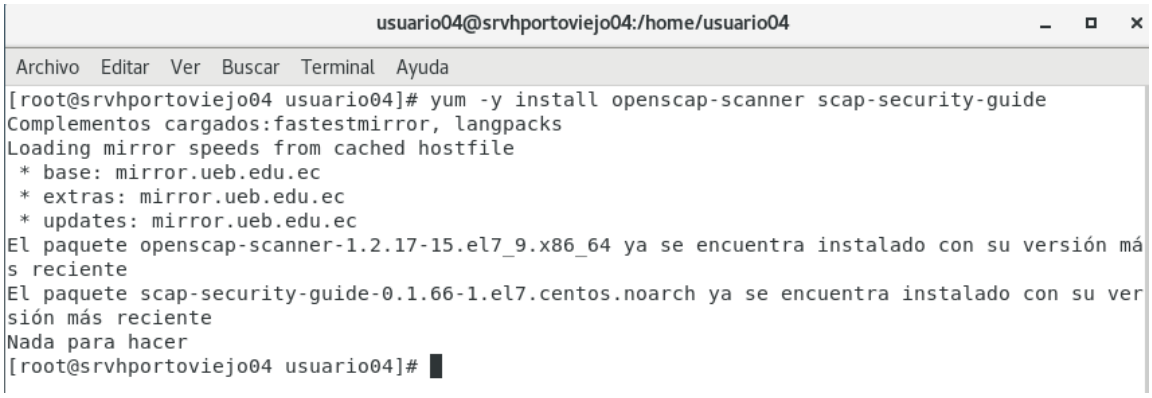


Ilustración 6. Instalación de OpenSCAP en Servidor del Hospital General Portoviejo

Ilustración 7. Perfiles disponibles de OpenSCAP en Servidor del Hospital General Portoviejo

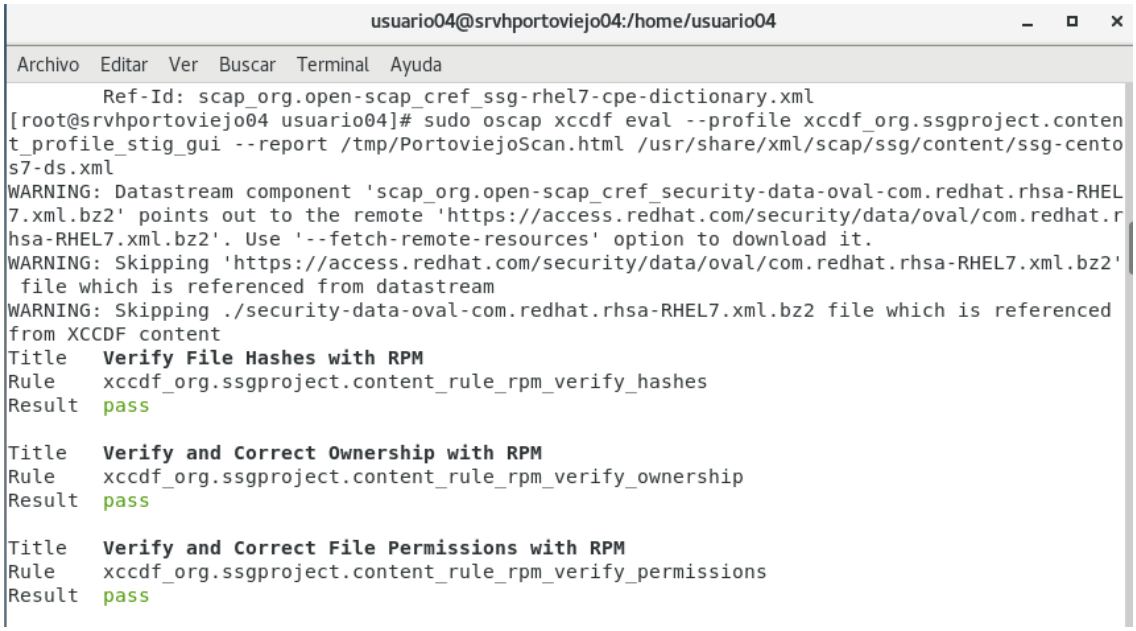


Ilustración 8. Escaneo de vulnerabilidades en los servidores del Hospital General Portoviejo

Instalación de OpenSCAP en los servidores del Hospital General Manta.

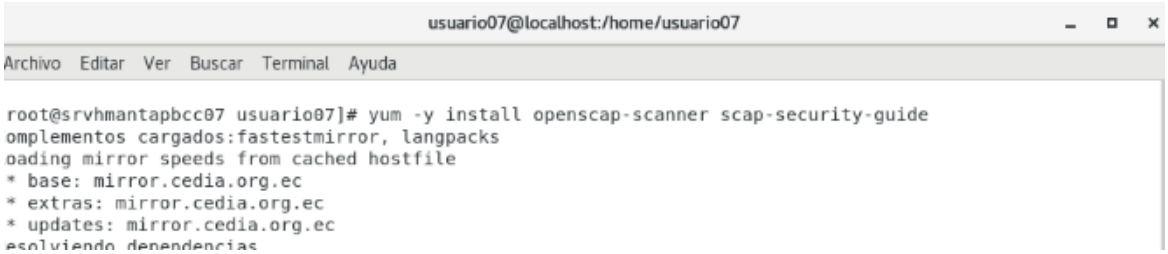


Ilustración 9. Instalación de OpenSCAP en Servidor del Hospital General Manta

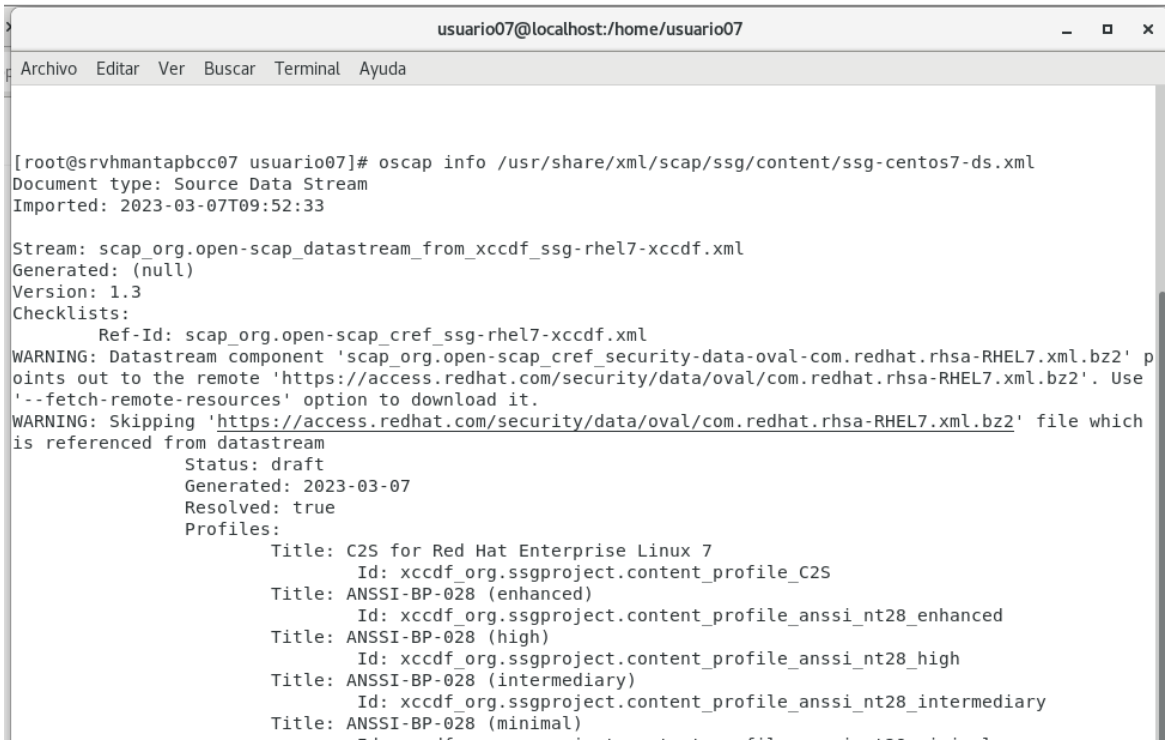


Ilustración 10. Perfiles disponibles de OpenSCAP en Servidor del Hospital General Manta

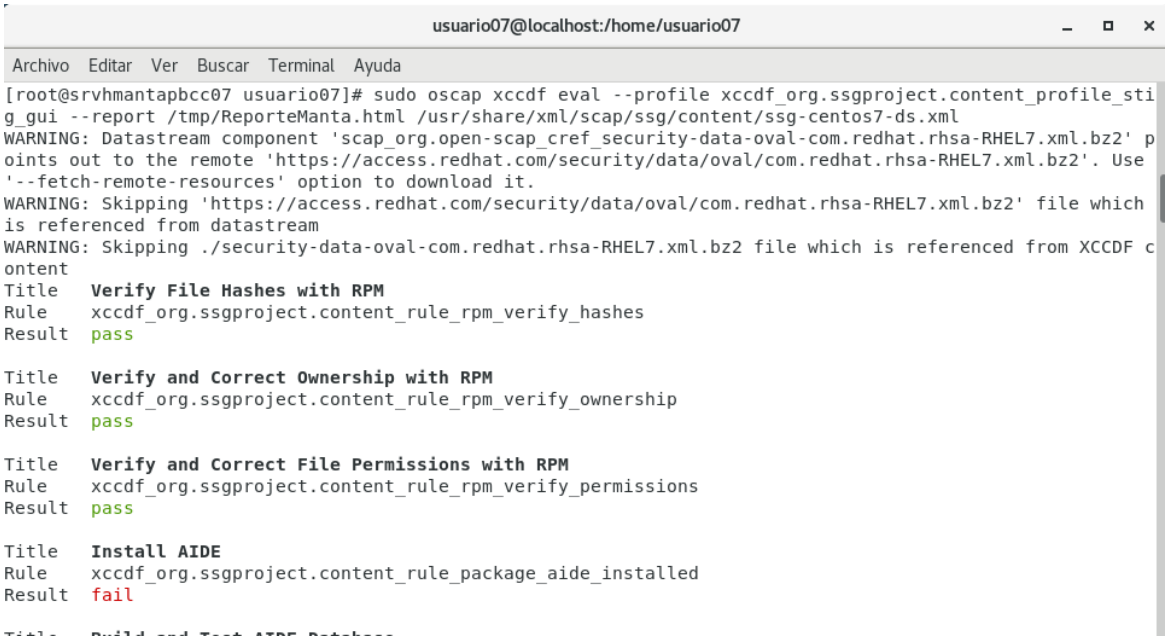


Ilustración 11. *Escaneo de vulnerabilidades en los servidores del Hospital General Manta*

3.9.2. Análisis de resultados de los escaneos realizados.

Para el cumplimiento de este objetivo vamos a dirigirnos a la ubicación que especificamos al momento de realizar el escaneo de vulnerabilidades ya que tendremos como resultado un archivo.html con los resultados obtenidos de cada Hospital

- Resultados del Escaneo realizado en el Hospital Básico Chone

Ilustración 12. *Resultados del Escaneo de vulnerabilidades del servidor del Hospital Básico Chone*

Ilustración 13. *Vulnerabilidad 1 Verificación de Archivos Hash con RPM*

Deshabilitar el acceso SSH a través de contraseñas vacías ✕

ID de regla	xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-sshd_disable_empty_passwords:def:1
Tiempo	2023-05-19T11:54:57
Gravedad	alto
Identificadores y Referencias	Referencias: NT007(R17) , PR.AC-4 , PR.AC -6 , PR.DS-5 , PR.IP-1 , PR.PT-3 , 11 , 12 , 13 , 14 , 15 , 16 , 18 , 3 , 5 , 9 , SV-204425r603261_rule , CCI-000366 , CCI-000766 , SR 1.1 , SR 1.10 , SR 1.11 , SR 1.12 , SR 1.13 , SR 1.2. RS 7.6 , 5.5 _ .6 , 164.308(a)(4)(i) , 164.308(b)(1) , 164.308(b)(3) , 164.310(b) , 164.312(e)(1) , 164.312(e)(2) (ii) ,SRG-OS-000480-VMM-002000 , SRG-OS-000106-GPOS-00053 , SRG-OS-000480-GPOS-00229 , SRG-OS-000480-GPOS-00227 , 4.3.3.2.2 , 4.3.3.5 1 , 4.3.3.5.2 , 4.3.3.5.3 , 4.3.3.5.4 , 4.3.3.5.5 , 4.3.3.5.6 , 4.3.3.5.7 , 4.3.3.5.8 , 4.3.3.6.1 , 4.3.3.6.2 , 4.3.3.6.3 , 4.3.3.6.4 , 4.3.3.6.5 , 4.3.3.6.6 , 4.3.3.6.7 , 4.3.3.6.8 , 4.3.3.6.9, 4.3.3.7.1 , 4.3.3.7.2 , 4.3.3.7.3 , 4.3.3.7.4 , 4.3.4.3.2 , 4.3.4.3.3 , FIA_UAU.1 , APO01.06 , BAI10.01 , BAI10 .02 , BAI10.03 , BAI10.05 , DSS05.02 , DSS05.04 , DSS05.05 , DSS05.07 , DSS06.02 , DSS06.03 , DSS06.06 , A.10.1.1 , A.11.1.4 , A.11.1.5 , A.11.2.1 ,A.12.1.2 , A.12.5.1 , A.12.6.2 , A.13.1.1 , A.13.1.3 , A.13.2.1 , A.13.2.3 , A.13.2.4 , A. 14.1.2 , A.14.1.3 , A.14.2.2 , A.14.2.3 , A.14.2.4 , A.6.1.2 , A.7.1.1 , A.7.1.2 , A.7.3. 1 , A.8.2.2 , A.8.2.3 , A.9.1.1 , A.9.1.2 , A.9.2.1 , A.9.2.3 , A.9.4.1 ,A.9.4.4 , A.9.4.5 , 5.3.11 , 3.1.1 , 3.1.5 , Req-2.2.6 , AC-17(a) , CM-7(a) , CM-7(b) , CM-6(a)
Descripción	No permitir el inicio de sesión SSH con contraseñas vacías. La configuración predeterminada de SSH deshabilita los inicios de sesión con contraseñas vacías. Se utiliza la configuración adecuada si no se establece ningún valor para `PermitEmptyPasswords` . Para prohibir explícitamente el inicio de sesión SSH desde cuentas con contraseñas vacías, agregue o corrija la siguiente línea en

Ilustración 14. *Vulnerabilidad 2. Acceso mediante SSH a través de contraseña vacía Activado*

Desinstalar el paquete vsftpd ✕

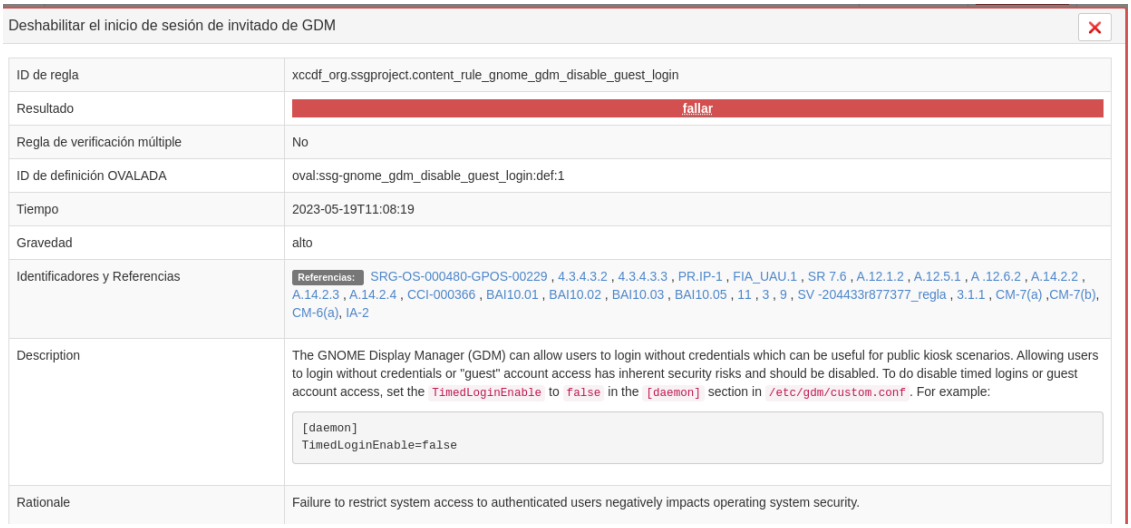
ID de regla	xccdf_org.ssgproject.content_rule_package_vsftpd_removed
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-paquete_vsftpd_removed:def:1
Tiempo	2023-05-19T11:54:48
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000074-GPOS-00042 , SRG-OS-000095-GPOS-00049 , SRG-OS-000480-GPOS-00227 , 4.3.3.5.1 , 4.3.3.5.2 , 4.3.3.5.3 , 4.3.3.5.4 , 4.3.3.5.5 , 4.3.3.5.6 , 4.3.3.5.7 , 4.3.3.5.8 , 4.3.3.6.1 , 4.3.3.6.2 , 4.3.3.6.3 , 4.3 . 3.6.4 , 4.3.3.6.5 , 4.3.3.6.6 , 4.3.3.6.7 , 4.3.3.6.8 , 4.3.3.6.9 , 4.3.3.7.1 ,4.3.3.7.2 , 4.3.3.7.3 , 4.3.3.7.4 , 4.3.4.3.2 , 4.3.4.3.3 , PR.IP-1 , PR.PT -3 , SR 1.1 , SR 1.10 , SR 1.11 , SR 1.12 , SR 1.13 , SR 1.2 , SR 1.3 , SR 1.4 , SR 1.5 , SR 1.6, SR 1.7, SR 1.8 , SR 1.9 , SR 2.1 , SR 2.2 , SR 2.3 , SR 2.4 , SR 2.5, SR 2.6 , SR 2.7 , SR 7.6 , A.12.1.2 , A.12.5.1 , A.12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , A.9.1. 2 , 2.2.8 , CCI-000197 , CCI-000366 , CCI-000381 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , DSS05.02 , DSS05.05 , DSS06.06 , 11 , 14 , 3 ,9 , Req-2.2.4 , SV-204620r603261_rule , CM-7(a) , CM-7(b) , CM-6(a) , IA-5(1)(c) , IA-5(1). 1(v) , CM-7 , CM-7.1(ii)
Descripción	El `vsftpd` paquete se puede eliminar con el siguiente comando: `$ sudo yum borrar vsftpd`
Razón fundamental	Quitar el `vsftpd` paquete disminuye el riesgo de su activación accidental

Ilustración 15.Paquete vsftpd Instalado

Desinstalar el paquete telnet-server ✕

ID de regla	xccdf_org.ssgproject.content_rule_package_telnet-server_removed
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-package_telnet-server_removed:def:1
Tiempo	2023-05-19T11:54:57
Gravedad	alto
Identificadores y Referencias	Referencias: BP28(R1) , SRG-OS-000095-GPOS-00049 , 4.3.3.5.1 , 4.3.3.5.2 , 4.3.3.5.3 , 4.3.3.5.4 , 4.3.3.5.5 , 4.3.3.5 .6 , 4.3.3.5.7 , 4.3.3.5.8 , 4.3.3.6.1 , 4.3.3.6.2 , 4.3.3.6.3 , 4.3.3.6.4 , 4.3.3.6.5 , 4.3.3.6.6 , 4.3.3.6.7 , 4.3.3.6.8 , 4.3.3.6.9 , 4.3.3.7.1 , 4.3.3.7.2 , 4.3.3.7.3 ,4.3.3.7.4 , 4.3.4.3.2 , 4.3.4.3.3 , PR.AC-3 , PR.IP-1 , PR.PT-3 , PR.PT-4 , APO13.01 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , DSS01.04 , DSS05.02 , DSS05.03 , DSS05.05 , DSS06.06 , A.11.2.6 , A.12.1.2 , A.12.5.1 , A.12.6.2 , A.13.1.1 , A.13.2.1 , A.14.1.3, A.14.2.2 , A.14.2.3 , A.14.2.4 , A.6.2.1 , A.6.2.2 , A.9.1.2 , 2.2.15 , CCI-000381 , SR 1.1 , SR 1.10 . _SR 2.4 , SR 2.5 , SR 2.6 , SR 2.7 , SR 3.1 , SR 3.5 , SR 3.8 , SR 4.1 , SR 4.3 , SR 5.1 , SR 5.2 , SR 5.3 , SR 7.1 , SR 7.6 , 11 , 12 , 14 , 15 , 3 , 8 , 9 , Req-2.2.4 , SV-204502r603261_rule , 164.308(a)(4)(i) , 164.308(b)(1) ,164.308(b)(3) , 164.310(b) , 164.312(e)(1) , 164.312(e)(2)(ii) , CM-7(a) , CM-7(b) , CM-6(a)
Descripción	El `telnet-server` paquete se puede eliminar con el siguiente comando: `$ sudo yum borrar servidor telnet`

Ilustración 16. *Paquete telnet-server instalado*



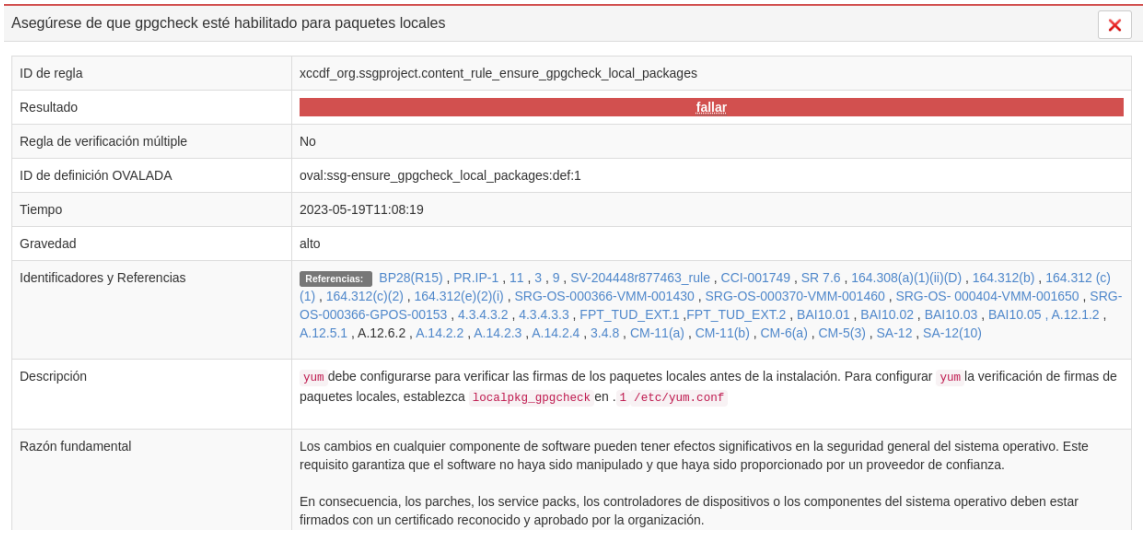
Deshabilitar el inicio de sesión de invitado de GDM

ID de regla	xccdf_org.ssgproject.content_rule_gnome_gdm_disable_guest_login
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-gnome_gdm_disable_guest_login:def:1
Tiempo	2023-05-19T11:08:19
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00229 , 4.3.4.3.2 , 4.3.4.3.3 , PR.IP-1 , FIA_UAU.1 , SR 7.6 , A.12.1.2 , A.12.5.1 , A .12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , CCI-000366 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , 11 , 3 , 9 , SV -204433r877377_regla , 3.1.1 , CM-7(a) ,CM-7(b), CM-6(a), IA-2

Description	The GNOME Display Manager (GDM) can allow users to login without credentials which can be useful for public kiosk scenarios. Allowing users to login without credentials or "guest" account access has inherent security risks and should be disabled. To do disable timed logins or guest account access, set the `TimedLoginEnable` to `false` in the `[daemon]` section in `/etc/gdm/custom.conf`. For example:
	`[daemon]`
	`TimedLoginEnable=false`

Rationale	Failure to restrict system access to authenticated users negatively impacts operating system security.

Ilustración 17. *Inicio de sesión de invitado GDM Activado*



Asegúrese de que gpgcheck esté habilitado para paquetes locales

ID de regla	xccdf_org.ssgproject.content_rule_ensure_gpgcheck_local_packages
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-ensure_gpgcheck_local_packages:def:1
Tiempo	2023-05-19T11:08:19
Gravedad	alto
Identificadores y Referencias	Referencias: BP28(R15) , PR.IP-1 , 11 , 3 , 9 , SV-204448r877463_rule , CCI-001749 , SR 7.6 , 164.308(a)(1)(ii)(D) , 164.312(b) , 164.312 (c)(1) , 164.312(c)(2) , 164.312(e)(2)(i) , SRG-OS-000366-VMM-001430 , SRG-OS-000370-VMM-001460 , SRG-OS- 000404-VMM-001650 , SRG-OS-000366-GPOS-00153 , 4.3.4.3.2 , 4.3.4.3.3 , FPT_TUD_EXT.1 ,FPT_TUD_EXT.2 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , A.12.1.2 , A.12.5.1 , A.12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , 3.4.8 , CM-11(a) , CM-11(b) , CM-6(a) , CM-5(3) , SA-12 , SA-12(10)
Descripción	`yum` debe configurarse para verificar las firmas de los paquetes locales antes de la instalación. Para configurar `yum` la verificación de firmas de paquetes locales, establezca `localpkg_gpgcheck` en . `1 /etc/yum.conf`
Razón fundamental	Los cambios en cualquier componente de software pueden tener efectos significativos en la seguridad general del sistema operativo. Este requisito garantiza que el software no haya sido manipulado y que haya sido proporcionado por un proveedor de confianza. En consecuencia, los parches, los service packs, los controladores de dispositivos o los componentes del sistema operativo deben estar firmados con un certificado reconocido y aprobado por la organización.

Ilustración 18. *gpgcheck habilitado para paquetes locales*

- Resultados del Escaneo en el Hospital General Portoviejo

Ilustración 19. Resultados del Escaneo de vulnerabilidades del servidor del Hospital General Portoviejo

Ilustración 20. Nombre de Usuario administrador del cargador de arranque en un valor no permitido

Deshabilitar la secuencia de teclas de reinicio Ctrl-Alt-Del en GNOME3

ID de regla	xccdf_org.ssgproject.content_rule_dconf_gnome_disable_ctrlaltdel_reboot
Resultado	fallar
Regla de verificación múltiple	no
ID de definición OVALADA	oval:ssg-dconf_gnome_disable_ctrlaltdel_reboot:def:1
Tiempo	2023-05-17T09:14:15
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00227 , 4.3.3.7.3 , PR.AC-4 , PR.DS-5 , SR 2.1 , SR 5.2 , A.10.1.1 , A.11.1.4 , A. 11.1.5 , A.11.2.1 , A.13.1.1 , A.13.1.3 , A.13.2.1 , A.13.2.3 , A.13.2.4 , A.14.1.2 , A.14.1. 3 , A.6.1.2 , A.7.1.1 , A.7.1.2 , A.7.3.1 , A.8.2.2 , A.8.2.3 ,A.9.1.1 , A.9.1.2 , A.9.2.3 , A.9.4.1 , A.9.4.4 , A.9.4.5 , CCI-000366 , APO01.06 , DSS05.04 , DSS05 . 07 , DSS06.02 , 12 , 13 , 14 , 15 , 16 , 18 , 3 , 5 , SV-204456r603261_regla , 3.1.2 , CM-6(a) , AC-6(1) , CM-7(b)

Descripción	De manera predeterminada, `GNOME` reiniciará el sistema si `Ctrl-Alt-Del` se presiona la secuencia de teclas.
	Para configurar el sistema para que ignore la secuencia de teclas de la interfaz gráfica de `Ctrl-Alt-Del` usuario (GUI) en lugar de reiniciar el sistema, agregue o configure `logout` en . Por ejemplo: `'' /etc/dconf/db/local.d/00-security-settings`
	`[org/gnome/settings-daemon/plugins/media-keys]`
	`cerrar sesión=''`
	Una vez que se hayan agregado las configuraciones, agregue un bloqueo `/etc/dconf/db/local.d/locks/00-security-settings-lock` para evitar la modificación del usuario. Por ejemplo:
	`/org/gnome/settings-daemon/plugins/media-keys/logout`
	Después de establecer la configuración, ejecute `dconf update` .

Razón fundamental	A locally logged-in user who presses Ctrl-Alt-Del, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

Ilustración 21. *Secuencia de teclas de reinicio Ctrl+Alt+Dep en GNOME3 Habilitado*

Deshabilitar el inicio de sesión automático de GDM

ID de regla	xccdf_org.ssgproject.content_rule_gnome_gdm_disable_automatic_login
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-gnome_gdm_disable_automatic_login:def:1
Tiempo	2023-05-17T09:14:14
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00229 , 4.3.4.3.2 , 4.3.4.3.3 , PR.IP-1 , FIA_UAU.1 , SR 7.6 , A.12.1.2 , A.12.5.1 , A .12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , CCI-000366 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , 11 , 3 , 9 , SV -204432r877377_regla , 3.1.1 , CM-6(a) ,AC-6(1) , CM-7(b)

Descripción	GNOME Display Manager (GDM) puede permitir que los usuarios inicien sesión automáticamente sin la interacción del usuario o las credenciales. Siempre se debe solicitar al usuario que se autentique en el sistema que está autorizado a usar. Para deshabilitar la capacidad del usuario para iniciar sesión automáticamente en el sistema, establezca `AutomaticLoginEnable` en `false` la `[daemon]` sección en `/etc/gdm/custom.conf` . Por ejemplo:
	`[daemon]`
	`AutomaticLoginEnable=falso`

Razón fundamental	No restringir el acceso al sistema a los usuarios autenticados afecta negativamente la seguridad del sistema operativo.

Ilustración 22. *Inicio de Sesión automático de GDM Activado*

Deshabilitar el acceso SSH a través de contraseñas vacías

ID de regla	xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-sshd_disable_empty_passwords:def:1
Tiempo	2023-05-17T09:21:08
Gravedad	alto
Identificadores y Referencias	Referencias: NT007(R17) , PR.AC-4 , PR.AC -6 , PR.DS-5 , PR.IP-1 , PR.PT-3 , 11 , 12 , 13 , 14 , 15 , 16 , 18 , 3 , 5 , 9 , SV-204425r603261_rule , CCI-000366 , CCI-000766 , SR 1.1 , SR 1.10 , SR 1.11 , SR 1.12 , SR 1.13 , SR 1.2. RS 7.6 , 5.5 _ .6 , 164.308(a)(4)(i) , 164.308(b)(1) , 164.308(b)(3) , 164.310(b) , 164.312(e)(1) , 164.312(e)(2) (ii) ,SRG-OS-000480-VMM-002000 , SRG-OS-000106-GPOS-00053 , SRG-OS-000480-GPOS-00229 , SRG-OS-000480-GPOS-00227 , 4.3.3.2.2 , 4.3.3.5 1 , 4.3.3.5.2 , 4.3.3.5.3 , 4.3.3.5.4 , 4.3.3.5.5 , 4.3.3.5.6 , 4.3.3.5.7 , 4.3.3.5.8 , 4.3.3.6.1 , 4.3.3.6.2 , 4.3.3.6.3 , 4.3.3.6.4 , 4.3.3.6.5 , 4.3.3.6.6 , 4.3.3.6.7 , 4.3.3.6.8 , 4.3.3.6.9, 4.3.3.7.1 , 4.3.3.7.2 , 4.3.3.7.3 , 4.3.3.7.4 , 4.3.4.3.2 , 4.3.4.3.3 , FIA_UAU.1 , APO01.06 , BAI10.01 , BAI10 .02 , BAI10.03 , BAI10.05 , DSS05.02 , DSS05.04 , DSS05.05 , DSS05.07 , DSS06.02 , DSS06.03 , DSS06.06 , A.10.1.1 , A.11.1.4 , A.11.1.5 , A.11.2.1 ,A.12.1.2 , A.12.5.1 , A.12.6.2 , A.13.1.1 , A.13.1.3 , A.13.2.1 , A.13.2.3 , A.13.2.4 , A. 14.1.2 , A.14.1.3 , A.14.2.2 , A.14.2.3 , A.14.2.4 , A.6.1.2 , A.7.1.1 , A.7.1.2 , A.7.3. 1 , A.8.2.2 , A.8.2.3 , A.9.1.1 , A.9.1.2 , A.9.2.1 , A.9.2.3 , A.9.4.1 ,A.9.4.4 , A.9.4.5 , 5.3.11 , 3.1.1 , 3.1.5 , Req-2.2.6 , AC-17(a) , CM-7(a) , CM-7(b) , CM-6(a)
Descripción	No permitir el inicio de sesión SSH con contraseñas vacías. La configuración predeterminada de SSH deshabilita los inicios de sesión con contraseñas vacías. Se utiliza la configuración adecuada si no se establece ningún valor para `PermitEmptyPasswords` . Para prohibir explícitamente el inicio de sesión SSH desde cuentas con contraseñas vacías, agregue o corrija la siguiente línea en `/etc/ssh/sshd_config` : `PermitEmptyPasswords no` Cualquier cuenta con contraseñas vacías debe deshabilitarse de inmediato y la configuración de PAM debe evitar que los usuarios puedan asignarse contraseñas vacías.
Razón fundamental	La configuración de esta configuración para el demonio SSH proporciona una garantía adicional de que el inicio de sesión remoto a través de SSH requerirá una contraseña, incluso en el caso de una configuración incorrecta en otro lugar.

Ilustración 23. *Acceso a SSH mediante contraseñas vacías Activado*

Ilustración 24. *gpgcheck deshabilitado para paquete locales*

Ilustración 25. *Inicio de Sesión en cuentas con contraseñas vacías Activado*

- Resultados del Escaneo en el Hospital General Manta

Ilustración 26. Resultados del Escaneo de vulnerabilidades del servidor del Hospital General Manta

Ilustración 27. *Vuln. 1 Hospital General Manta - Inicio de Sesión en cuentas con contraseñas vacías*

Ilustración 28. *Vuln. 2 Hospital General Manta - Nombre de usuario administrador del cargador de arranque en un valor no permitido*

Ilustración 29. *Vuln 3 Hospital General Manta - Contraseña del Cargador de arranque en grub2 no establecido*

Deshabilitar la secuencia de teclas de reinicio Ctrl-Alt-Del en GNOME3

ID de regla	xccdf_org.ssgproject.content_rule_dconf_gnome_disable_ctrlaltdel_reboot
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-dconf_gnome_disable_ctrlaltdel_reboot:def:1
Tiempo	2023-05-18T20:10:17
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00227 , 4.3.3.7.3 , PR.AC-4 , PR.DS-5 , SR 2.1 , SR 5.2 , A.10.1.1 , A.11.1.4 , A. 11.1.5 , A.11.2.1 , A.13.1.1 , A.13.1.3 , A.13.2.1 , A.13.2.3 , A.13.2.4 , A.14.1.2 , A.14.1. 3 , A.6.1.2 , A. 7.1.1 , A.7.1.2 , A.7.3.1 , A.8.2.2 , A.8.2.3 ,A.9.1.1 , A.9.1.2 , A.9.2.3 , A.9.4.1 , A.9.4.4 , A.9.4.5 , CCI-000366 , APO01.06 , DSS05.04 , DSS05 . 07 , DSS06.02 , 12 , 13 , 14 , 15 , 16 , 18 , 3 , 5 , SV-204456r603261_regla , 3.1.2 , CM-6(a) , AC-6(1) , CM-7(b)
Descripción	De manera predeterminada, GNOME reiniciará el sistema si Ctrl-Alt-Del se presiona la secuencia de teclas. Para configurar el sistema para que ignore la secuencia de teclas de la interfaz gráfica de Ctrl-Alt-Del usuario (GUI) en lugar de reiniciar el sistema, agregue o configure logout en . Por ejemplo: '' /etc/dconf/db/local.d/00-security-settings [org/gnome/settings-daemon/plugins/media-keys] cerrar sesión='' Una vez que se hayan agregado las configuraciones, agregue un bloqueo /etc/dconf/db/local.d/locks/00-security-settings-lock para evitar la modificación del usuario. Por ejemplo: /org/gnome/settings-daemon/plugins/media-keys/logout Después de establecer la configuración, ejecute dconf update .
Razón fundamental	Un usuario conectado localmente que presiona Ctrl-Alt-Del, cuando está en la consola, puede reiniciar el sistema. Si se presiona accidentalmente, como podría suceder en el caso de un entorno de sistema operativo mixto, esto puede crear el riesgo de pérdida de disponibilidad a corto plazo de los sistemas debido a un reinicio involuntario.

Ilustración 30. *Vuln 4 Hospital General Manta - Secuencia de teclas de reinicio Ctrl+Alt+Del en GNOME3 Activado*

Deshabilitar el inicio de sesión de invitado de GDM

ID de regla	xccdf_org.ssgproject.content_rule_gnome_gdm_disable_guest_login
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-gnome_gdm_disable_guest_login:def:1
Tiempo	2023-05-18T20:10:17
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00229 , 4.3.4.3.2 , 4.3.4.3.3 , PR.IP-1 , FIA_UAU.1 , SR 7.6 , A.12.1.2 , A.12.5.1 , A .12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , CCI-000366 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , 11 , 3 , 9 , SV -204433r877377_regla , 3.1.1 , CM-7(a) ,CM-7(b) , CM-6(a) , IA-2
Descripción	GNOME Display Manager (GDM) puede permitir que los usuarios inicien sesión sin credenciales, lo que puede ser útil para escenarios de quioscos públicos. Permitir que los usuarios inicien sesión sin credenciales o acceso a una cuenta de "invitado" tiene riesgos de seguridad inherentes y debe deshabilitarse. Para deshabilitar los inicios de sesión programados o el acceso a la cuenta de invitado, establezca TimedLoginEnable en false la [daemon] sección en /etc/gdm/custom.conf . Por ejemplo: [daemon] TimedLoginEnable=falso
Razón fundamental	No restringir el acceso al sistema a los usuarios autenticados afecta negativamente la seguridad del sistema operativo.

Ilustración 31. *Vuln 5 Hospital General Manta - Inicio de Sesión de invitado de GDM Habilitado*

Deshabilitar el inicio de sesión automático de GDM

ID de regla	xccdf_org.ssgproject.content_rule_gnome_gdm_disable_automatic_login
Resultado	fallar
Regla de verificación múltiple	No
ID de definición OVALADA	oval:ssg-gnome_gdm_disable_automatic_login:def:1
Tiempo	2023-05-18T20:10:17
Gravedad	alto
Identificadores y Referencias	Referencias: SRG-OS-000480-GPOS-00229 , 4.3.4.3.2 , 4.3.4.3.3 , PR.IP-1 , FIA_UAU.1 , SR 7.6 , A.12.1.2 , A.12.5.1 , A .12.6.2 , A.14.2.2 , A.14.2.3 , A.14.2.4 , CCI-000366 , BAI10.01 , BAI10.02 , BAI10.03 , BAI10.05 , 11 , 3 , 9 , SV -204432r877377_regla , 3.1.1 , CM-6(a) ,AC-6(1) , CM-7(b)
Descripción	GNOME Display Manager (GDM) puede permitir que los usuarios inicien sesión automáticamente sin la interacción del usuario o las credenciales. Siempre se debe solicitar al usuario que se autentique en el sistema que está autorizado a usar. Para deshabilitar la capacidad del usuario para iniciar sesión automáticamente en el sistema, establezca AutomaticLoginEnable en false la [daemon] sección en /etc/gdm/custom.conf . Por ejemplo: [daemon] AutomaticLoginEnable=falso
Razón fundamental	No restringir el acceso al sistema a los usuarios autenticados afecta negativamente la seguridad del sistema operativo.

Ilustración 32. *Vuln 6 Hospital General Manta - Inicio de sesión automático de GDM Habilitado*

Ilustración 33. *Vul 7. Hospital General Manta - Acceso a través de SSH con contraseñas vacías Habilitado*

3.9.3. Desarrollo e implementación de medidas de seguridad recomendadas en base a resultados obtenidos por OpenSCAP

- Medidas correctivas aplicadas en el Hospital Básico Chone.

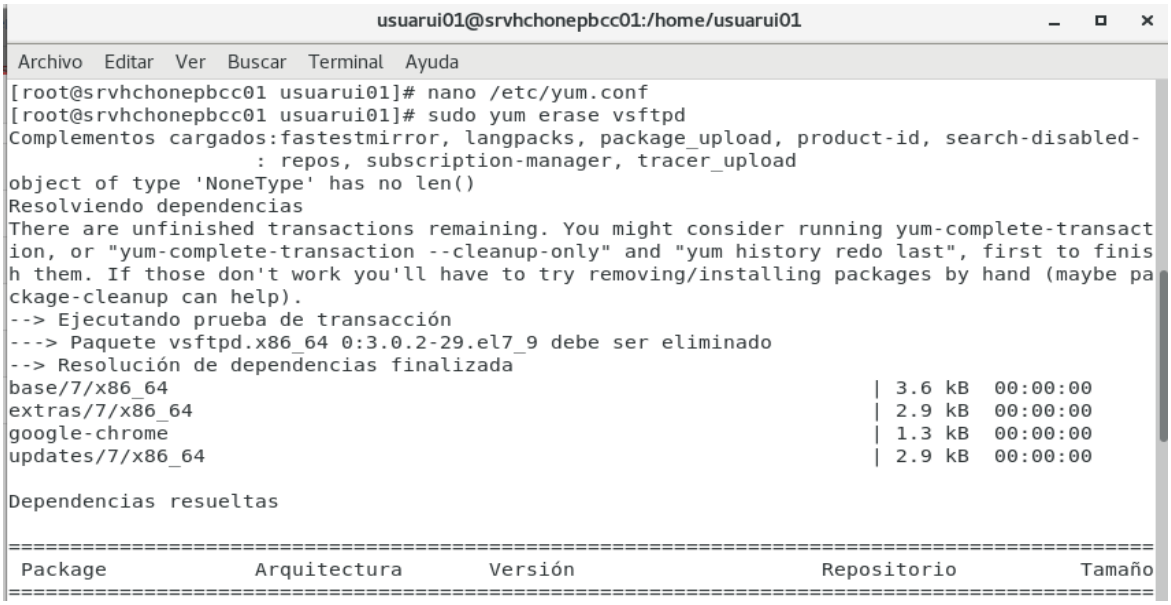


Ilustración 34. *Desinstalación del Paquete vsftpd - Hospital Básico Chone*

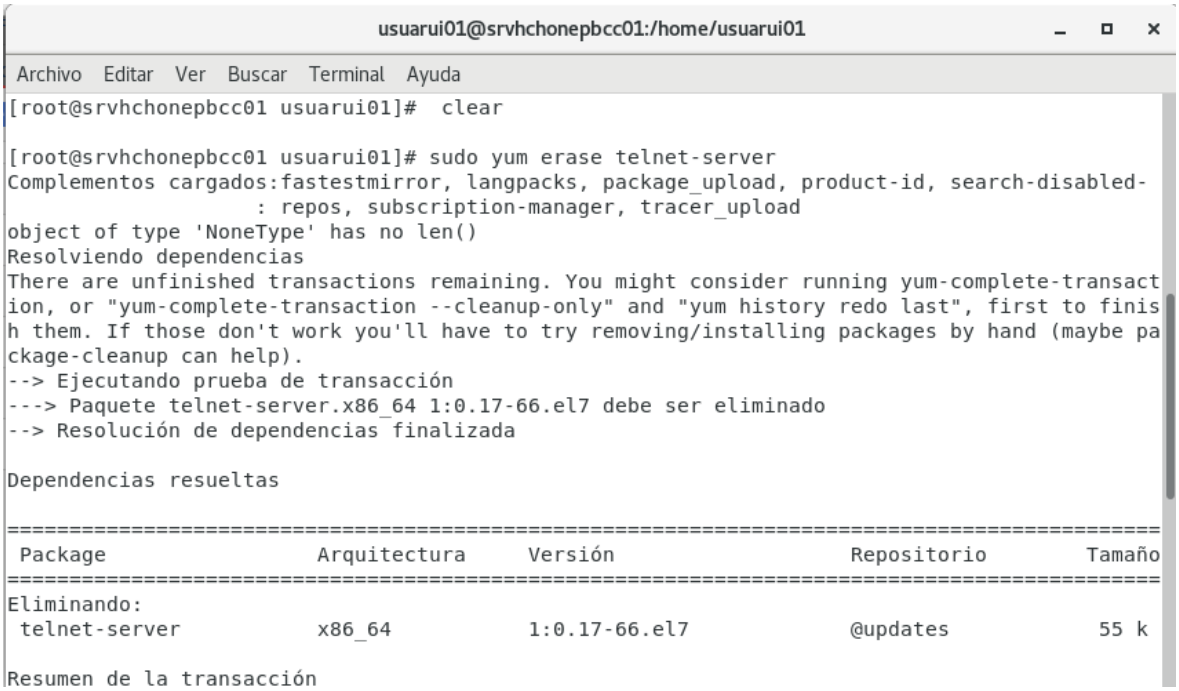


Ilustración 35. *Desinstalación de paquetes Telnet-Server*

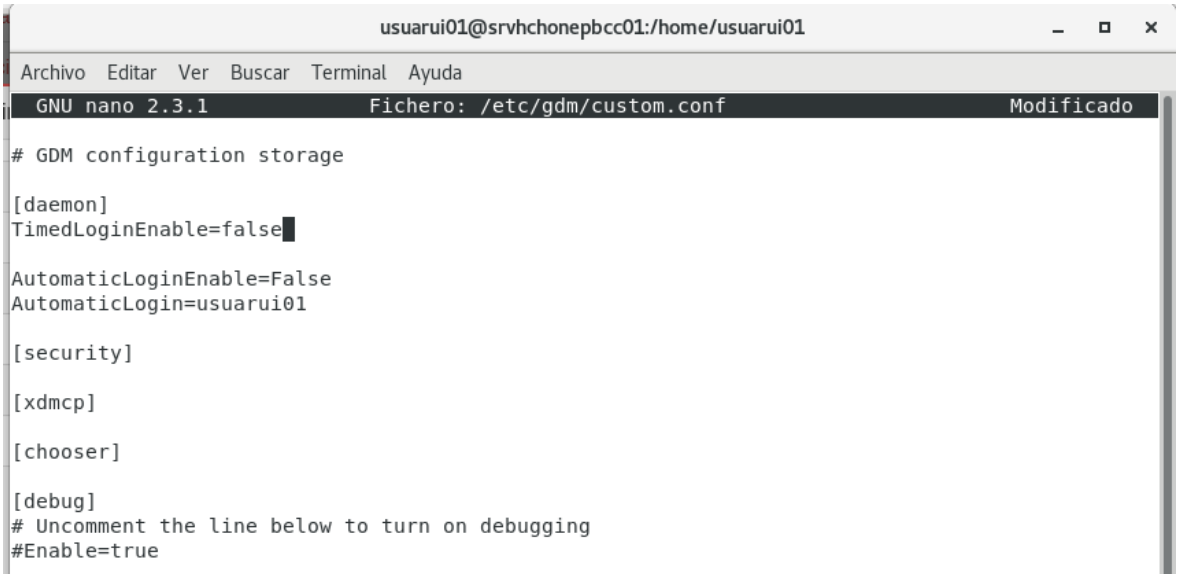


Ilustración 36. *Inicio de sesión de invitado GDM Desactivado*

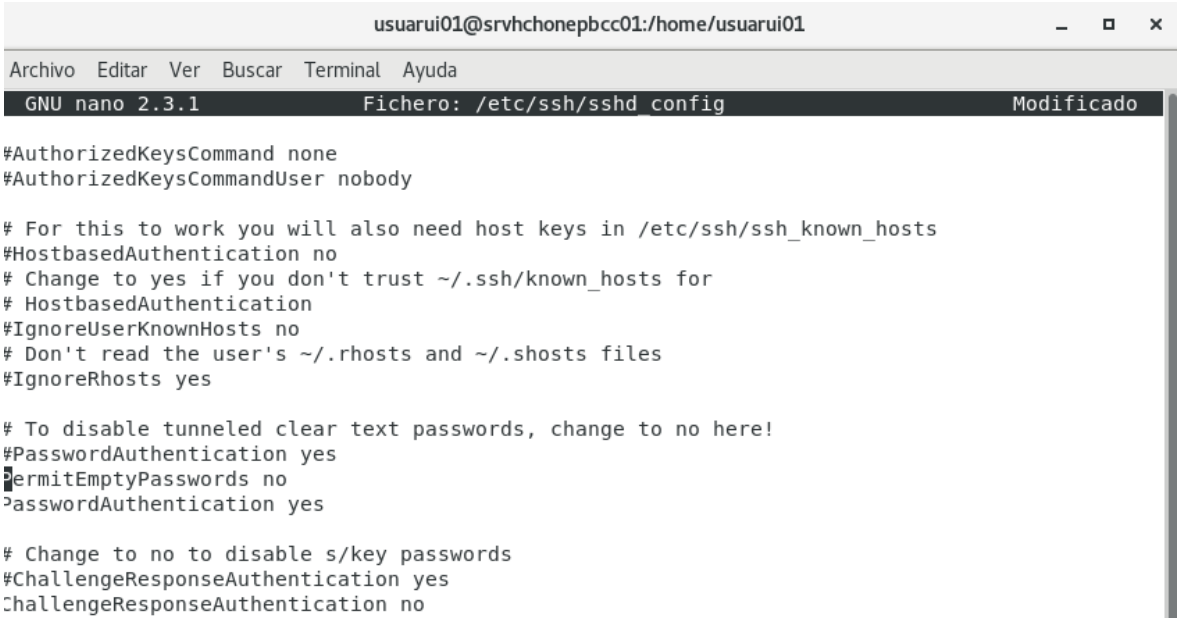


Ilustración 37. *Acceso a SSH mediante contraseñas vacías Desactivado*

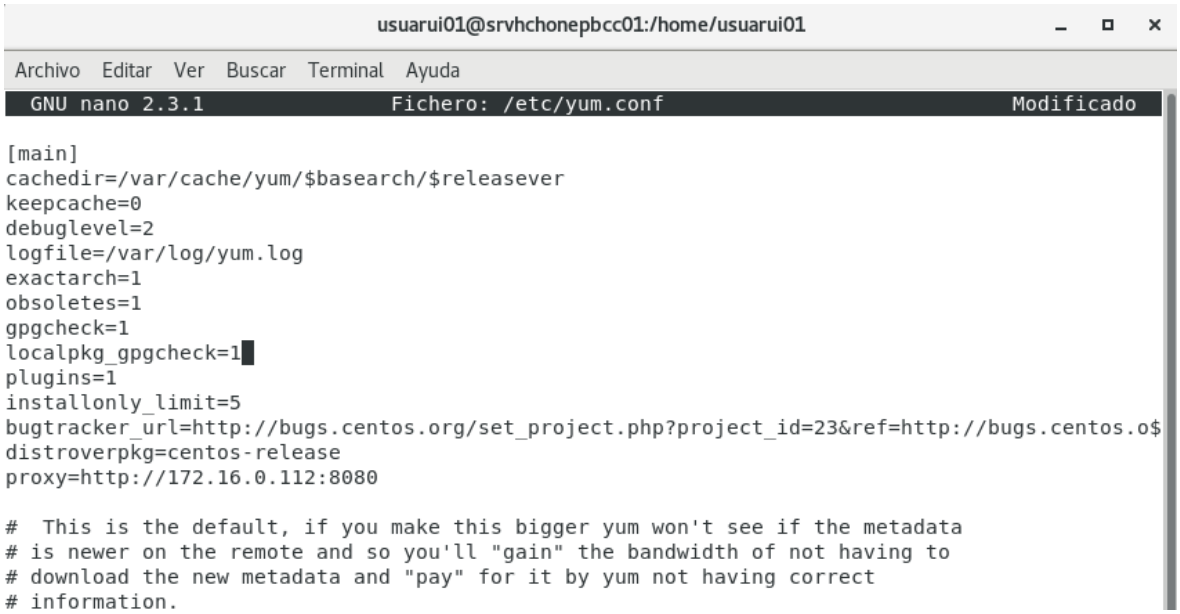


Ilustración 38. *gpgcheck para paquetes locales Habilitado*

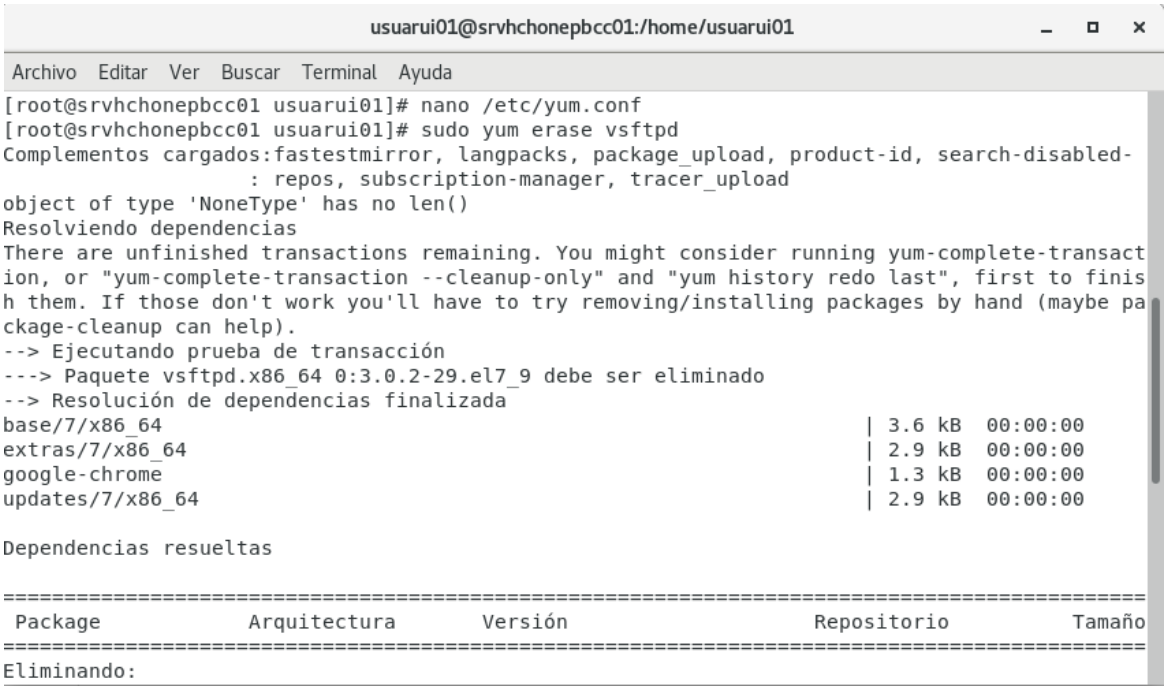


Ilustración 39. *Paquete vsftpd Desinstalado*

- Medidas correctivas aplicadas en el Hospital Portoviejo

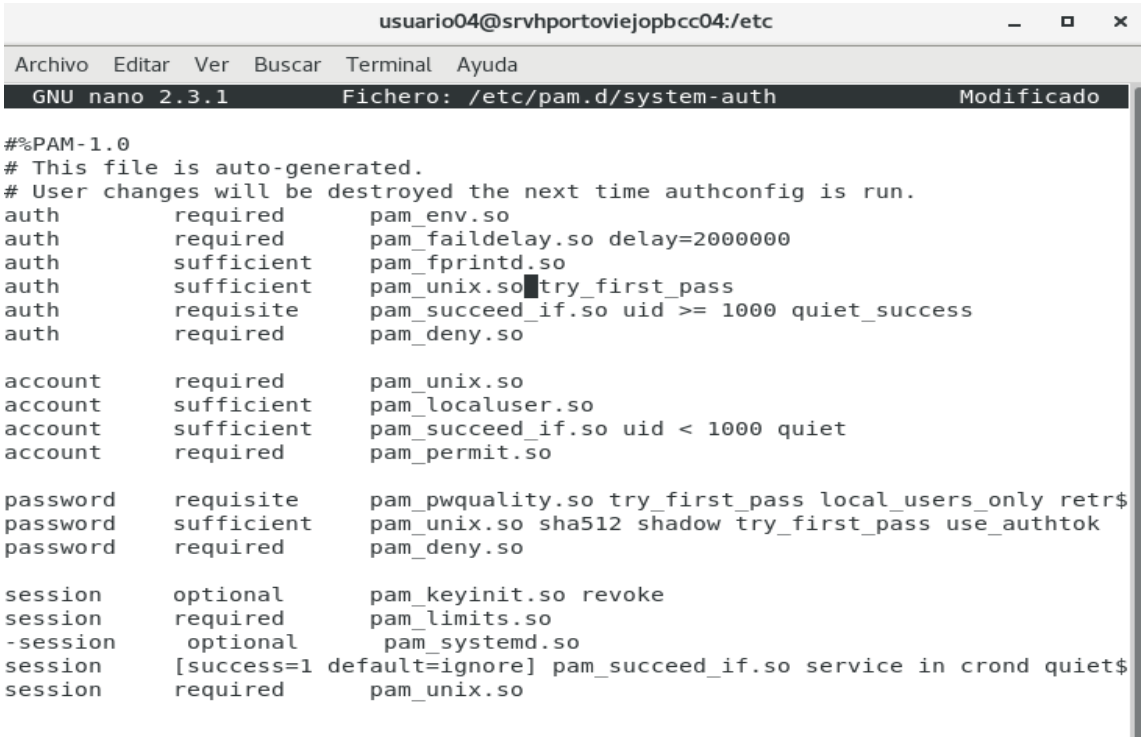


Ilustración 40*. Inicio de Sesión en cuentas vacías Desactivado*

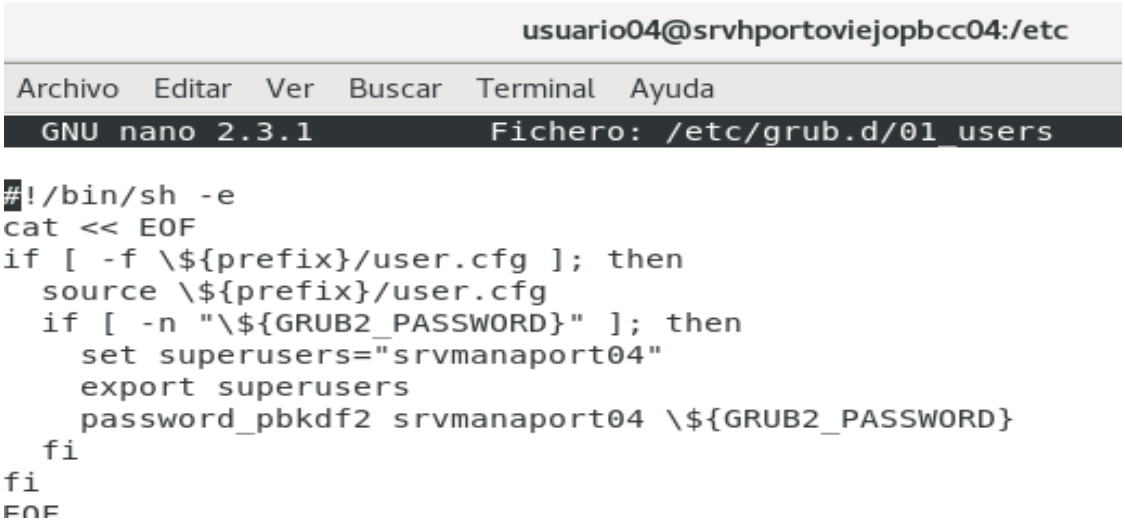


Ilustración 41. *Nombre de usuario de administrador del cargador de arranque*

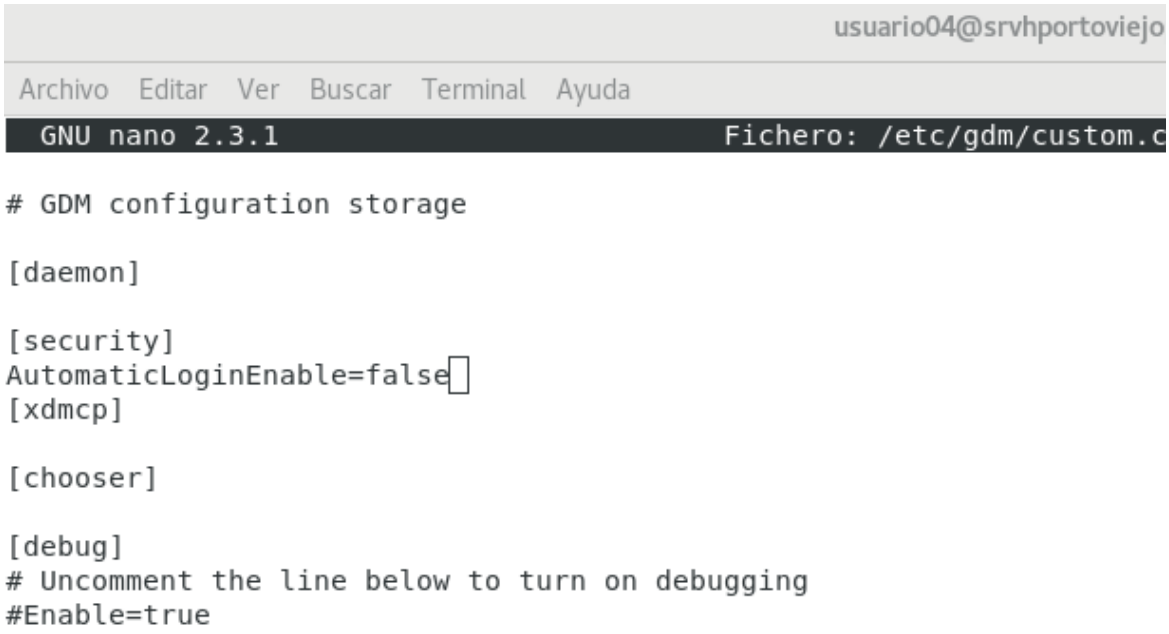


Ilustración 42. *Inicio de sesión desactivado en GDM*

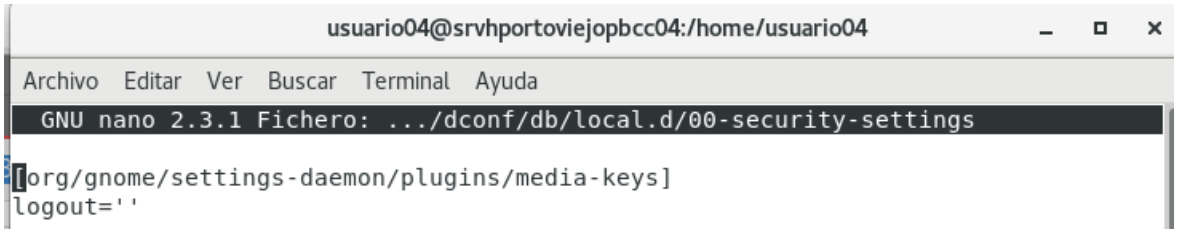


Ilustración 43. *Secuencia de teclas de reinicio Ctrl-Alt-Del Deshabilitado*

- Medidas correctivas aplicadas en el Servidor de Manta

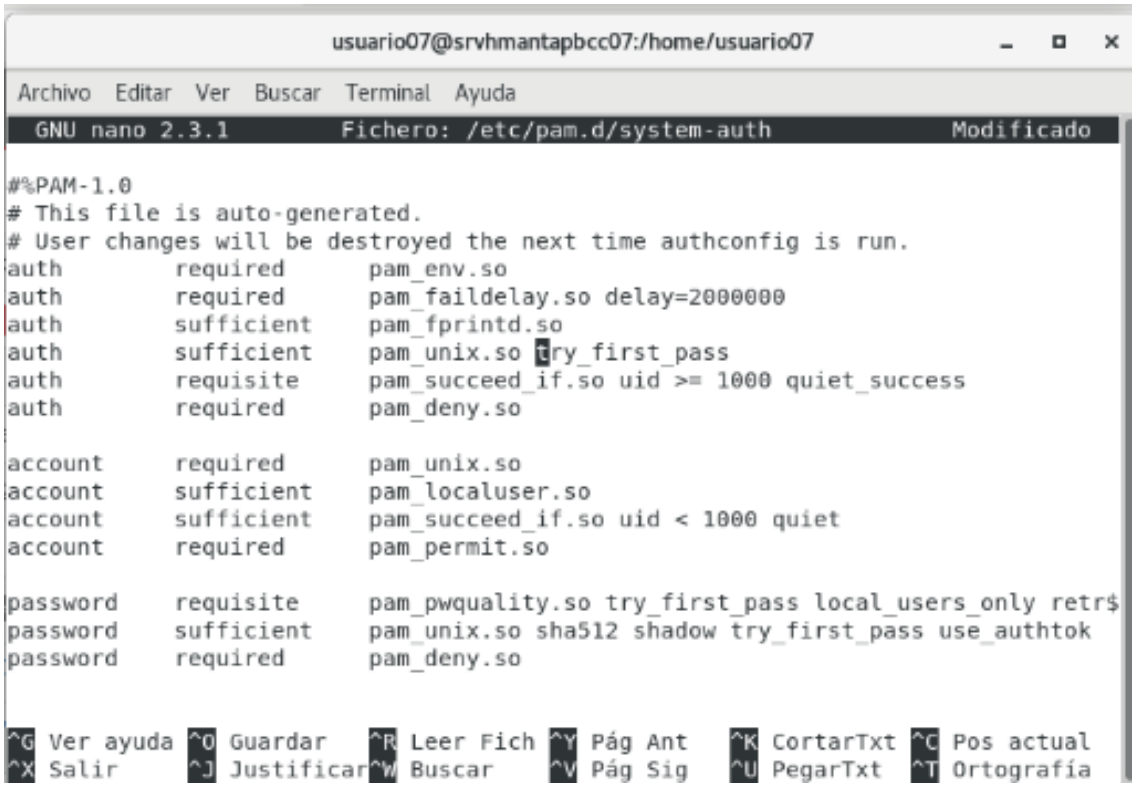


Ilustración 44. *Impedir inicio de sesión de cuentas con contraseñas vacias*

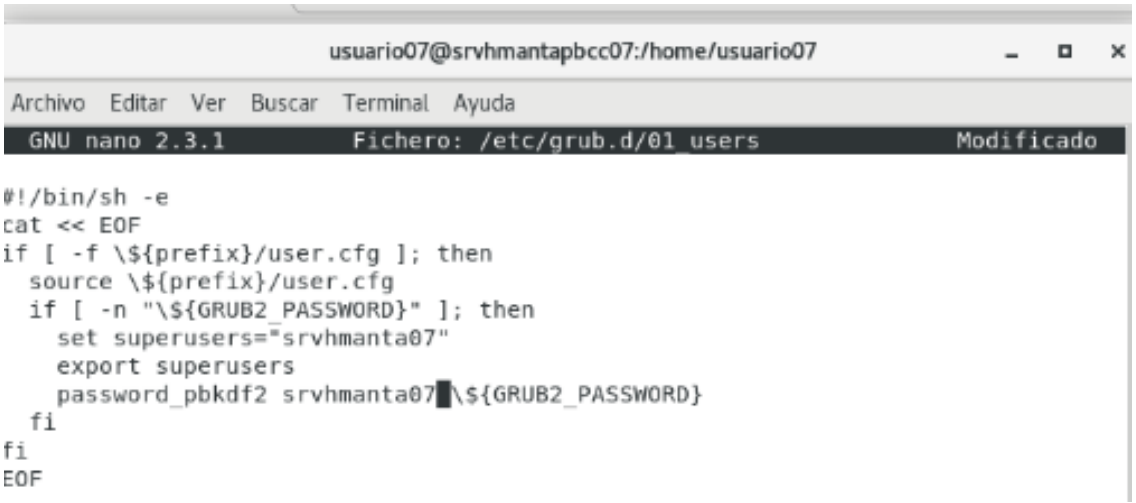


Ilustración 45*. Configuración de nombre de usuario administrador del cargador de arranque*

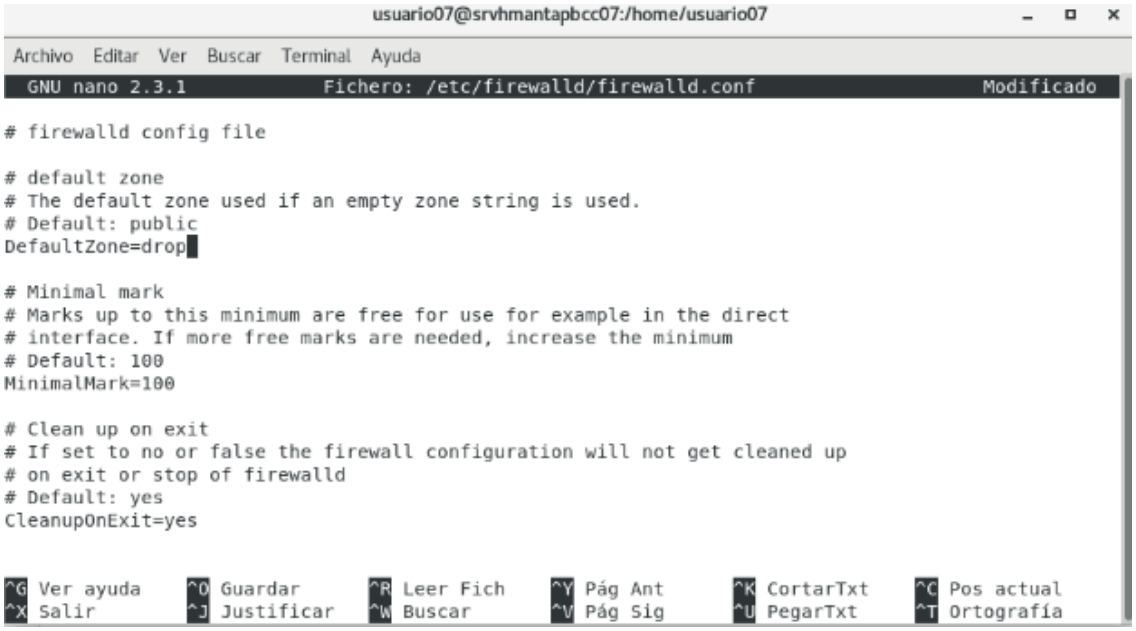


Ilustración 46. *Configuración de zona de firewall predeterminada para paquetes entrantes*

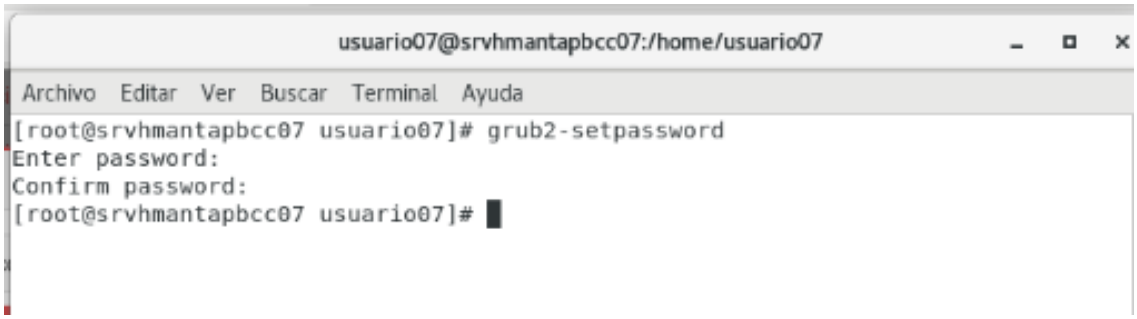


Ilustración 47. *Contraseña del cargador de arranque en grub2 establecida*

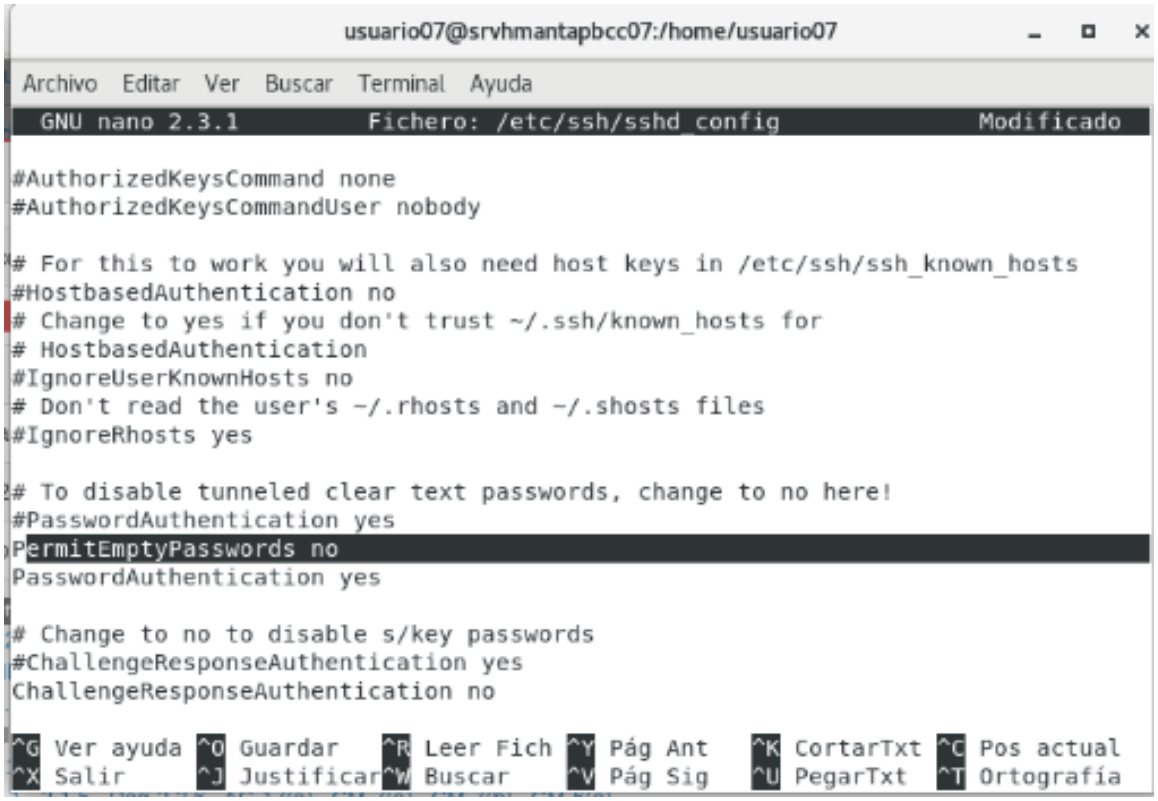


Ilustración 48. *Acceso SSH a través de contraseñas vacías desactivado*

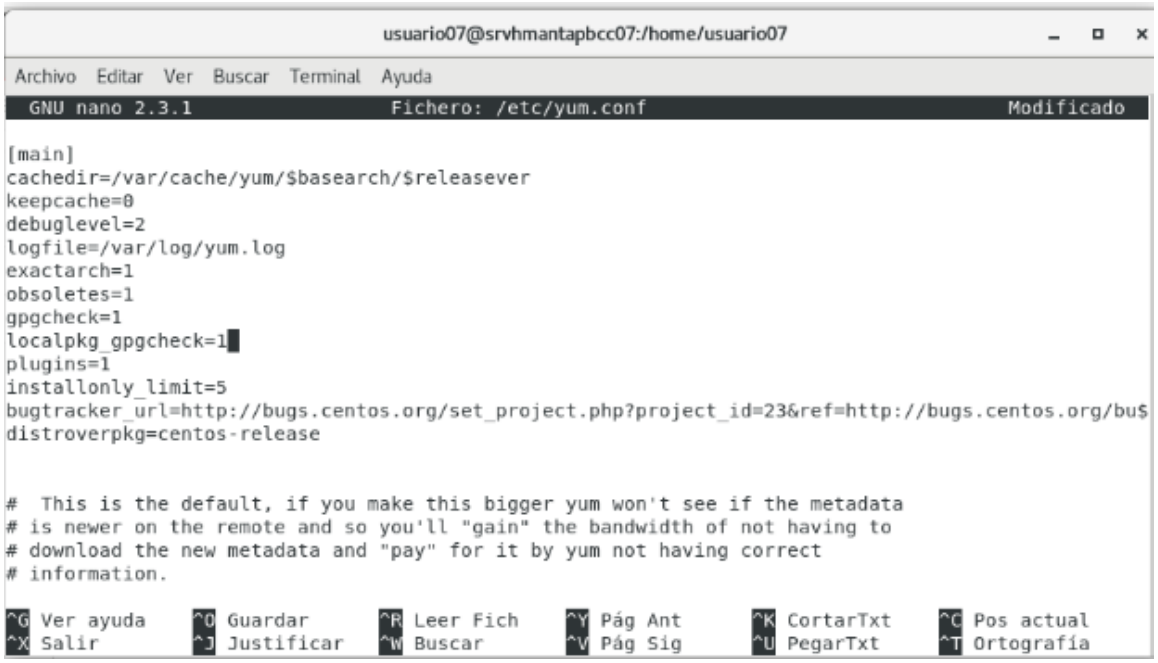


Ilustración 49. *Gpgcheck habilitado para paquetes locales*

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Durante el proceso de escaneo de vulnerabilidades utilizando OpenSCAP en los servidores de los hospitales del IESS en la provincia de Manabí, se identificaron diversas vulnerabilidades en los sistemas. A continuación, se presentan los resultados obtenidos:

Se detectaron un total de 45 vulnerabilidades de alta gravedad, 486 vulnerabilidades de gravedad media y 30 vulnerabilidades de baja gravedad en los servidores analizados. Estas vulnerabilidades abarcaban diferentes áreas, como configuraciones inseguras, falta de parches de seguridad, contraseñas débiles, entre otros.

Las vulnerabilidades más comunes encontradas fueron: Acceso SSH a través de contraseñas vacías, Contraseña del cargador de arranque en grub2 sin configurar, Nombre de usuario administrador del cargador de arranque en un valor no predeterminado sin configurar, Inicio de sesión de invitado de GDM habilitado, gpgcheck habilitado para paquetes locales, Paquete vsftpd habilitado, lo que representó un riesgo significativo para la seguridad de los servidores y la confidencialidad de la información almacenada en ellos.

4.2. DISCUSIÓN

La identificación de estas vulnerabilidades críticas en los servidores de los hospitales del IESS resalta la importancia de fortalecer la ciberseguridad en estos entornos. A continuación, se discuten los hallazgos y las acciones tomadas para corregir las vulnerabilidades identificadas:

Se implementó un plan de acción inmediato para abordar las vulnerabilidades críticas identificadas durante los escaneos. Se priorizaron aquellas que representaban el mayor riesgo y se asignaron los recursos necesarios para su corrección.

Se realizaron las siguientes acciones correctivas para abordar las vulnerabilidades identificadas:

Actualización de los sistemas operativos y aplicaciones a las versiones más recientes que incluyen los parches de seguridad necesarios.

Implementación de políticas de contraseñas robustas y su aplicación en todos los usuarios y cuentas de acceso.

Tras la implementación de estas correcciones, se realizó un nuevo escaneo de vulnerabilidades para evaluar la efectividad de las acciones correctivas. Los resultados mostraron una disminución significativa en el número de vulnerabilidades detectadas y un aumento en el nivel general de seguridad de los servidores.

En conclusión, el análisis de vulnerabilidades realizado mediante OpenSCAP permitió identificar y corregir las vulnerabilidades existentes en los servidores de los hospitales del IESS. La implementación de las acciones correctivas adecuadas ha mejorado la seguridad de los servidores y ha reducido el riesgo de posibles ataques y filtraciones de información confidencial.

Es importante destacar que la ciberseguridad debe ser un proceso continuo y en constante evolución. Se recomienda mantener una vigilancia activa, realizar actualizaciones periódicas y llevar a cabo auditorías de seguridad regulares para garantizar la protección continua de los sistemas y la información sensible.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La implementación de un sistema de ciberseguridad basado en una biblioteca de código abierto, como OpenSCAP, es una estrategia efectiva para identificar y corregir vulnerabilidades en los servidores de los hospitales. Los escaneos de vulnerabilidades realizados permitieron detectar una variedad de debilidades en los sistemas, lo que resalta la importancia de contar con medidas de seguridad robustas.

- Las vulnerabilidades identificadas en los servidores de los hospitales representaban un riesgo significativo para la confidencialidad, integridad y disponibilidad de la información almacenada. La implementación de acciones correctivas, siguiendo las recomendaciones de los informes de OpenSCAP, permitió fortalecer la seguridad de los servidores y reducir el riesgo de posibles ataques y filtraciones de datos sensibles.

- La ciberseguridad debe ser un enfoque integral y continuo en los entornos hospitalarios. Además de implementar herramientas de análisis de vulnerabilidades, es crucial mantener una política de seguridad sólida que incluya actualizaciones regulares de software, configuraciones seguras, prácticas de autenticación robustas y capacitación del personal en aspectos de seguridad cibernética

5.2. RECOMENDACIONES

- Es recomendable establecer un programa de monitoreo y gestión de seguridad cibernética en los hospitales, que incluya la realización periódica de escaneos de vulnerabilidades utilizando herramientas como OpenSCAP. Esto permitirá identificar y abordar oportunamente las nuevas vulnerabilidades que puedan surgir debido a actualizaciones de software, configuraciones erróneas o nuevas amenazas emergentes.

- Se recomienda implementar una política de parcheo regular y oportuna para los sistemas operativos y aplicaciones utilizados en los servidores de los hospitales. Mantenerse actualizado con las últimas actualizaciones de seguridad y parches de software es fundamental para mitigar riesgos y proteger los sistemas contra vulnerabilidades conocidas.

- Es esencial proporcionar capacitación continua en seguridad cibernética al personal de los hospitales, tanto a nivel técnico como a nivel de usuarios finales. La concienciación sobre las mejores prácticas de seguridad, como el uso de contraseñas robustas, la protección de dispositivos y la detección de intentos de phishing, contribuirá a crear una cultura de seguridad sólida y a reducir los riesgos asociados con el factor humano.

BIBLIOGRAFÍA

Avila Pesantez, D., Chalan Analuisa, R., Figueras, G., & Avila, M. (29 de Junio de 2022). *VIII INTERNATIONALCONGRESS OF SCIENCE TECHNOLOGY ENTREPRENEURSHIP AND INNOVATION (SECTEI 2021)*. Recuperado el 21 de Abril de 2023, de Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study: https://www.researchgate.net/profile/Diego-Avila-Pesantez/publication/361618445_Cybersecurity_Policies_for_Network_Switching_Devices_in_Hospital_Data_Centers_A_Case_Study_Politicas_de_Ciberseguridad_para_los_Dispositivos_de_Conmutacion_de_Red_en_el_Centro

Benjamin, F., D. Kyle, M., Taylor, J., & Clemens Scott, K. (sf de sf de 2019). *Cybersecurity in healthcare: A systematic review of modern threats and trends*. Recuperado el 21 de Abril de 2023, de Cybersecurity in healthcare: A systematic review of modern threats and trends: https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263

Carrera, R. (27 de Junio de 2019). *¿Qué es un servidor?* Recuperado el 25 de Febrero de 2023, de ¿Qué es un servidor?: https://hostingwebcloud.com/que-es-un-servidor/

Cornejo Montoya, Y., Verdezoto, V., & Villacís, A. (2019). Ciberdefensa, Ciberseguridad y sus efectos en la sociedad. *International Multilingual Journal of Science and Technology.*, 4. Recuperado el 21 de Abril de 2023

Federal Bureau of Investigatión. (sf de sf de 2021). *Internet Cime Complaint Center IC3*. Recuperado el 27 de 12 de 2022, de Annual Reports: https://www.ic3.gov/Home/AnnualReports

Greenbone Networks. (sf de sf de 2023). *OpenVAS - Escáner abierto de evaluación de vulnerabilidades*. Recuperado el 02 de 02 de 2023, de Greenbone OpenVAS: https://www.openvas.org/

Illa, R. (01 de 06 de 2019). *Seguridad en servidores empresariales*. Recuperado el 25 de 02 de 2023, de Seguridad en servidores empresariales: https://openaccess.uoc.edu/bitstream/10609/95326/6/rillagTFM0619memoria.pdf

INCIBE. (sf de sf de 2021). *Seguridad Informática*. Recuperado el 25 de Febrero de 2023, de Seguridad Informática: https://www.incibe.es/

Internet Crime Complaint Center (IC3). (sf de sf de 2021). *FEDERAL BUREAU OF INVESTIGATION*. Recuperado el 01 de Febrero de 2023, de Ransomware: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

ISO. (sf de sf de 2019). *Seguridad Informática*. Recuperado el 25 de Febrero de 2023, de Seguridad Informática: https://www.iso.org/home.html

ISO 27001. (s.f.). *NORMA ISO 27001*. Obtenido de NORMA ISO 27001: https://normaiso27001.es/

Laskos, A. (sf de sf de 2023). *Ecsypno – I+D y Consultoría*. Recuperado el 02 de 02 de 2023, de SCNR: https://ecsypno.com/

López, I. (28 de Mayo de 2019). *Herramientas para la gestión y análisis de Vulnerabilidades*. Recuperado el 02 de 02 de 2023, de ¿Qué son las herramientas de gestión y análisis de vulnerabilidades?: https://www.a2secure.com/blog/herramientas-para-la-gestion-y-analisis-de-vulnerabilidades/

Marcillo Parrales, K. (01 de Enero de 2021). *DETECCIÓN DE VULNERABILIDADES EN APLICACIONES WEB*. Recuperado el 21 de Abril de 2023, de ANÁLISIS DE LAS HERRAMIENTAS Y TÉCNICAS UTILIZADAS EN PRUEBA DE PENETRACIÓN PARA LA DETECCIÓN DE VULNERABILIDADES EN APLICACIONES WEB: https://revistas.unesum.edu.ec/index.php/unesumciencias/article/download/316/428/

NIST. (sf de sf de 2023). *SCAP*. Recuperado el 25 de Febrero de 2023, de ¿Que es SCAP?: https://www.nist.gov/

OpenSCAP. (sf de sf de 2023). *Herramientas*. Recuperado el 25 de 02 de 2023, de Herramientas: https://www.open-scap.org/

ORGANIZACIÓN INTERNACIONAL DE COMISIONES DE VALORES. (sf de sf de 2020). *Cyber Security in Securities Markets – An International Perspective.* Obtenido de Report on IOSCO's cyber risk coordination efforts : https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,. (17 de Abril de 2019). *Definición del término ciberseguridad.* Recuperado el 21 de Abril de 2023, de Definición del término ciberseguridad: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Red Hat. (sf de sf de 2023). *OpenScap*. Recuperado el 02 de 02 de 2023, de Herramientas: https://www.open-scap.org/

SANCHEZ MEDINA, I. (sf de sf de 2019). *UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD DE INGENIERÍAS*. Recuperado el 28 de 12 de 2022, de PROPUESTA DE INTERCEPTOR PROXY COMO MODELO DE ACCESO SEGURO A UN ENTORNO WEB, PARA EL CONSORCIO INFRAESTRUCTURA EDUCATIVA: https://repository.ucc.edu.co/bitstream/20.500.12494/7500/1/Propuesta%20Interceptor%20Proxy%20con%20squid.pdf

Sophos. (sf de sf de 2020). *Tendencias de Seguridad 2020*. Recuperado el 25 de Febrero de 2023, de Tendencias de Seguridad 2020: https://www.sophos.com/en-us?&cmp=78991&utm_campaign=GPD-2020-AMER-LATAM-PaidSearch-Google-SCH-B-Pure-Sophos-Exact-DG-78991&utm_medium=cpc&utm_content=B_Pure_Sophos_Exact&utm_term=Sophos&utm_source=google&gclid=CjwKCAiAxvGfBhB-EiwAMPakqoUCHG0l4SallVDOhTln

Subgraph. (sf de sf de 2023). *ESCÁNER DE VULNERABILIDADES VEGA*. Recuperado el 02 de 02 de 2023, de Vega lo ayuda a encontrar y corregir secuencias de comandos entre sitios (XSS), inyección de SQL: https://subgraph.com/vega/index.en.html

Surribas, N. (16 de 01 de 2023). Recuperado el 02 de 02 de 2023, de El escáner de vulnerabilidades de aplicaciones web: https://wapiti-scanner.github.io/

The Global Risks Report. (sf de sf de 2021). *Foro Económico Mundial*. Recuperado el 25 de Febrero de 2023, de The Global Risks Report: https://www.weforum.org/reports/global-risks-report-2023/

Troein, C., & Acayo, G. (08 de Octubre de 2020). *WTO Cybersecurity Webinar*. Recuperado el 02 de 02 de 2023, de ITU Global Cybersecurity Inde x: https://www.wto.org/english/res_e/reser_e/caroline_troein_and_grace_acoyo.pdf

ANEXOS

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Red Hat Enterprise Linux 7

with profile DISA STIG with GUI for Red Hat Enterprise Linux 7

— This profile contains configuration checks that align to the DISA STIG with GUI for Red Hat Enterprise Linux V3R10.

In addition to being applicable to Red Hat Enterprise Linux 7, DISA recognizes this configuration baseline as applicable to the operating system tier of Red Hat technologies that are based on Red Hat Enterprise Linux 7, such as:

- Red Hat Enterprise Linux Server
- Red Hat Enterprise Linux Workstation and Desktop
- Red Hat Enterprise Linux for HPC
- Red Hat Storage
- Red Hat Containers with a Red Hat Enterprise Linux 7 image

Warning: The installation and use of a Graphical User Interface (GUI) increases your attack vector and decreases your overall security posture. If your Information Systems Security Officer (ISSO) lacks a documented operational requirement for a graphical user interface, please consider using the standard DISA STIG for Red Hat Enterprise Linux 7 profile.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-

Anexo 1

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

This benchmark is a direct port of a *SCAP Security Guide* benchmark developed for *Red Hat Enterprise Linux*. It has been modified through an automated process to remove specific dependencies on *Red Hat Enterprise Linux* and to function with *CentOS*. The result is a generally useful *SCAP Security Guide* benchmark with the following caveats:

- *CentOS* is not an exact copy of *Red Hat Enterprise Linux*. There may be configuration differences that produce false positives and/or false negatives. If this occurs please file a bug report.
- *CentOS* has its own build system, compiler options, patchsets, and is a community supported, non-commercial operating system. *CentOS* does not inherit certifications or evaluations from *Red Hat Enterprise Linux*. As such, some configuration rules (such as those requiring *FIPS 140-2* encryption) will continue to fail on *CentOS*.

Members of the *CentOS* community are invited to participate in OpenSCAP and SCAP Security Guide development. Bug reports and patches can be sent to GitHub: https://github.com/ComplianceAsCode/content. The mailing list is at https://fedorahosted.org/mailman/listinfo/scap-security-guide.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Anexo 2

whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	srvhchonepbcc01
Benchmark URL	#scap_org.open-scap_comp_ssg-rhel7-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_stig_gui
Started at	2023-05-19T10:56:42
Finished at	2023-05-19T11:54:57
Performed by	usuarui01

CPE Platforms

- cpe:/o:centos:centos:7
- cpe:/o:redhat:enterprise_linux:7::client
- cpe:/o:redhat:enterprise_linux:7::computenod
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::server
- cpe:/o:redhat:enterprise_linux:7::workstation

Addresses

- IPv4 127.0.0.1
- IPv4 172.16.26.1
- IPv4 192.168.122.1
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:4bae:d9ef:d9b0:98da
- MAC 00:00:00:00:00:00
- MAC 2C:41:38:B8:D3:E7
- MAC 52:54:00:05:25:F3

Compliance and Scoring

The target system did not satisfy the conditions of 187 rules! Furthermore, the results of 1 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

Anexo 3

Rule results

67 passed | 187 failed | 8

Severity of failed rules

10 low | 162 medium | 15 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	48.745380	100.000000	48.75%

Rule Overview

pass, fail, notchecked, fixed, error, notapplicable, informational, unknown

Search through XCCDF rules — Search

Group rules by: Default

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux 7 — 187x fail, 1x error, 7x notchecked		
System Settings — 165x fail, 1x error, 7x notchecked		

Anexo 4