ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“IMPLEMENTACIÓN DE UN SISTEMA AUTOMATIZADO PARA EL REFORZAMIENTO CONTINUO DE LA SEGURIDAD EN SISTEMAS LINUX”

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

JUAN LEÓN MERA MEJÍA

MICHELLE IVETTE YAGER RODRÍGUEZ

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Primero a Dios, por guiarnos siempre y ayudarnos a tomar las mejores decisiones, a nuestras familias por el apoyo incondicional y a todos los profesionales con los que hemos compartido durante este proceso.

DEDICATORIA

A Dios, y a nuestras familias, por darnos siempre el impulso necesario para que estemos constantemente buscando lo mejor personal y profesionalmente.

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Eduardo Freire Cobo

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

Mgs. Juan C. García

REVISOR

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Trabajo de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

_____

JUAN LEÓN MERA MEJÍA

_____

MICHELLE IVETTE YAGER RODRÍGUEZ

RESUMEN

El presente trabajo de titulación tiene como objetivo principal el diseño y desarrollo de un prototipo de sistema automatizado para la evaluación y el fortalecimiento continuo de la seguridad en sistemas operativos Linux, ampliamente utilizados en pequeñas y medianas empresas (PYMES). El prototipo busca identificar y mitigar vulnerabilidades y configuraciones inseguras, preparando así a las organizaciones para su eventual implementación en entornos de producción.

El proyecto incluye un análisis exhaustivo del panorama tecnológico de las PYMES, identificando riesgos y amenazas asociados a las tecnologías utilizadas. A partir de este análisis, se desarrolla un plan de implementación que incorpora mejores prácticas de seguridad basadas en estándares reconocidos, con el fin de reforzar de manera continua las configuraciones de los sistemas Linux.

La validación del prototipo se realiza en un entorno controlado que simula la infraestructura de una PYME. Los resultados demuestran la efectividad del sistema en la reducción de vulnerabilidades y en la mejora de la seguridad, estableciendo una base sólida para su futura aplicación en entornos empresariales.

INDICE GENERAL

ABREVIATURAS

CIS	Center for Internet Security
NIST	National Institute of Standards and Technology
CLI	Command-Line Interface
IOT	Internet of Things
KASLR	Kernel Address Space Layout Randomization
KPTI	Kernel Page Table Isolation
TI	Tecnologías de la Información
PYME	Pequeñas y Medianas Empresas

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, donde la conectividad y la dependencia de la tecnología son omnipresentes, la seguridad de la información emerge como una prioridad crítica. Dentro de este marco, los servidores desempeñan una función crucial en la gestión de datos sensibles, convirtiéndose en objetivos prioritarios para amenazas cibernéticas. La implementación de medidas de seguridad efectivas resulta esencial para salvaguardar la integridad, confidencialidad y disponibilidad de los recursos almacenados en estos servidores. En este contexto, la noción de reforzamiento continuo de seguridad se presenta como una estrategia dinámica y proactiva para fortalecer la seguridad de los servidores.

La ciberseguridad se ha vuelto un componente esencial en entorno empresarial, donde las pequeñas y medianas empresas (PYMES) no permanecen ajenas a la creciente sofisticación de las amenazas cibernéticas. La presente tesis presenta un análisis del panorama tecnológico empleado por las PYMES, buscando identificar vulnerabilidades, riesgos y amenazas de seguridad inherentes a las tecnologías comúnmente utilizadas. Este análisis proporcionará una visión de la estrategia de ciberseguridad en las PYMES, sentando las bases para el diseño e implementación de un enfoque efectivo y proactivo para la protección de sistemas.

Como parte integral de este estudio, se propone un plan detallado de implementación destinado a evaluar el estado de configuración de los sistemas Linux, abordando de manera específica las recomendaciones de configuración basadas en estándares de seguridad reconocidos. Este enfoque tiene como objetivo proporcionar a las PYMES una guía práctica para fortalecer sus posturas de seguridad, ofreciendo no solo una

evaluación crítica de la situación actual, sino también recomendaciones concretas para mitigar riesgos y mejorar la resiliencia ante amenazas cibernéticas. Además, se busca implementar un sistema automatizado que permita la evaluación y el refuerzo continuo de las mejores prácticas de configuración a nivel de seguridad en los sistemas Linux, proporcionando una solución dinámica y proactiva para el mantenimiento de la seguridad informática en el entorno empresarial de las PYMES.

CAPÍTULO I

GENERALIDADES

1.1. Antecedentes

En la actualidad, debido a la creciente tendencia digital, se ha percibido un incremento en el mercado en línea por parte de las pequeñas y medianas empresas (PYMES). Con base en el reporte “The Future of Jobs Report” (World Economic Forum, 2023), más del 85% de las empresas reconocen que la mayor incorporación de tecnologías innovadoras y la expansión de la conectividad digital se consideran factores cruciales para promover procesos de transformación [1]. La infraestructura digital se ha identificado como un elemento fundamental que promueve el crecimiento económico a largo plazo y mejora la capacidad de adaptación de las PYMES.

Dentro de una gran variedad de estos entornos tecnológicos e informáticos utilizados por las pequeñas y medianas empresas persiste el sistema operativo Linux. Según las estadísticas de uso de sistemas operativos y servidores web (W3Techs, 2023), Linux es el sistema operativo fundamental para más del 81%

de los sitios web publicados y en 2021, se estimaba que alrededor del 90 % de las cargas de trabajo de la nube pública se ejecutaban en Linux.

La incorporación de este tipo de infraestructura digital y tecnológica por parte las pequeñas y medianas empresas acarrea el procesamiento información sensible, por lo cual, para cuidar de la seguridad de la información propia y de sus clientes, las PYMES deben cumplir con múltiples medidas y controles de seguridad que maximicen la protección de los datos.

De acuerdo con el reporte “Global Risk Report” (World Economic Forum, 2023), se posiciona al cibercrimen e inseguridad cibernética dentro de los riesgos más graves a nivel mundial durante la próxima década [2]. Las amenazas cibernéticas están experimentando una constante evolución, con un incremento en ataques más agresivos y avanzados que se aprovechan de una mayor exposición. Dentro de un entorno en que las PYMES se apoyan cada vez más en sistemas tecnológicos y digitales, el incremento de las amenazas cibernéticas está superando la capacidad de las comunidades para prevenirlas y gestionarlas de manera efectiva.

En consonancia con el informe The Linux Threat Landscape Report (Trend Micro, 2023), debido a la adopción generalizada en servidores empresariales e infraestructuras de nube, los sistemas Linux son un objetivo cada vez más atractivo para los actores maliciosos y las amenazas cibernéticas de tipo malware y explotación de vulnerabilidades. [3]

1.2. Descripción del Problema

Se evidencia que entre las principales debilidades aprovechadas por los

ciberatacantes como puntos de entrada fáciles en los sistemas Linux se encuentran la falta de actualización del sistema y la aplicación de configuraciones erróneas, dado que estas tareas suelen ejecutarse de forma manual con base al criterio o experiencia de los administradores de infraestructura y tecnología de las pequeñas y medianas empresas (PYMES).

Por lo antes expuesto, las PYMES que utilizan entornos tecnológicos e informáticos basados en sistemas operativos Linux y no implementen lineamientos de configuración robustos que prioricen la protección de datos mediante el cumplimiento sistemático de mejores prácticas de seguridad, pueden mantener vulnerabilidades en sus sistemas que pueden ser aprovechadas por atacantes externos para vulnerar los sistemas, causando daños económicos y reputacionales hacia las PYMES afectadas.

1.3. Solución Propuesta

El presente proyecto busca fortalecer la ciberseguridad de las PYMES que utilizan entornos tecnológicos e informáticos basados en sistemas operativos Linux, mitigando vulnerabilidades en los sistemas Linux y reduciendo la superficie de ataque ante los ciberdelincuentes. El reforzamiento automático y continuo de la seguridad en sistemas Linux permite verificar y corregir de forma autónoma la configuración actual de un sistema, con base al cumplimiento de los estándares de seguridad requeridos. [4]–[6]

La importancia del desarrollo de este tipo de sistema se justifica en virtud de la creciente complejidad y sofisticación de las amenazas cibernéticas y vulnerabilidades en la actualidad. [7], [8] La seguridad de los sistemas Linux es una preocupación primordial para las PYMES (pequeñas y medianas empresas).

Este tipo de organizaciones son los blancos más apetecibles para los actores maliciosos, debido a su falta de conocimiento y preparación técnica en materia de ciberseguridad, además de su presupuesto limitado para implementar soluciones de protección contra amenazas. [6], [7]

Esta automatización servirá como una herramienta valiosa para las PYMES que buscan proteger sus activos digitales, salvaguardar la integridad de los datos confidenciales y mantener la continuidad de sus operaciones en un entorno cibernético cada vez más hostil. Además, al facilitar la implementación y el seguimiento continuo de medidas de seguridad, esta solución será particularmente útil para los equipos de administración de sistemas y profesionales de ciberseguridad. [5], [6]

El presente proyecto reúne características técnicas y operativas que aseguran el cumplimiento de su objetivo, dado que los autores cuentan con los recursos tecnológicos necesarios para la implementación de la plataforma automatizada de evaluación y reforzamiento continuo de la seguridad en sistemas Linux, así como los conocimientos en postura de seguridad cibernética para garantizar cumplimiento de los estándares de seguridad requeridos. La implementación será factible realizarla en 4 meses.

1.4. Objetivo General

Diseñar y desarrollar un prototipo de sistema automatizado para la evaluación y fortalecimiento continuo de la seguridad en sistemas con distribuciones Linux ampliamente utilizadas en pequeñas y medianas empresas (PYMES), con el propósito de identificar y mitigar vulnerabilidades y riesgos de seguridad, contribuyendo a la preparación para una eventual implementación en entornos de producción y empresariales.

1.5. Objetivos Específicos

- Analizar el panorama tecnológico utilizado por las PYMES, identificando vulnerabilidades, riesgos y amenazas de seguridad asociados a las tecnologías utilizadas, para comprender la estrategia de ciberseguridad.

- Diseñar un plan detallado de implementación que evalúe el estado de configuración del sistema Linux e incorpore las recomendaciones de configuración específicas basadas en estándares de seguridad reconocidos.

- Desarrollar un prototipo de sistema automatizado para la evaluación y reforzamiento continuo de las mejores prácticas de configuración a nivel de seguridad en los sistemas Linux en entornos PYMES, como preparación para su posible implementación futura.

1.6. Metodología

El presente proyecto corresponde a un estudio no experimental, de tipo transversal, debido a que se evaluará el estado de seguridad basado en el cumplimiento de los requerimientos definidos por el estándar de seguridad CIS, para un grupo de servidores Linux dentro de un entorno de prueba controlado. La medición de cumplimiento de seguridad se realizará en el grupo de servidores Linux previa y posteriormente a la ejecución del sistema automatizado para el reforzamiento continuo de seguridad, para comparar los resultados.

Se utilizará como sujeto de estudio un grupo de servidores Linux implementados dentro de un entorno de prueba controlado, el cual simulará la infraestructura de tecnología de una pequeña empresa.

El entorno controlado constará de las siguientes características:

- Ambiente virtualizado: Utilizará tecnologías de virtualización para creación y gestión de máquinas virtuales (VM), las cuales conformarán los servidores.

- Réplica de entorno de producción: Reflejará configuración y características similares a los sistemas que se encuentran en entornos de producción en términos de sistemas operativos.

- Ambiente aislado: Se encontrará aislado de cualquier entorno de producción, garantizando la seguridad de las pruebas.

- Seguridad de acceso: Contará con medidas de seguridad para controlar y restringir el acceso a usuarios autorizados para la ejecución de la prueba.

Como instrumento se utilizará las métricas de cumplimiento con base a los N puntos de referencia definidos por el estándar de seguridad CIS. Los puntos de referencia abarcarán verificaciones de configuraciones de seguridad de los sistemas operativos Linux más utilizados.

Cabe destacar, que el número de puntos de referencia definidos por guía CIS varía dependiendo de los siguientes factores del sistema:

- Tipo de sistema operativo
- Versión de sistema operativo
- Tipo de distribución
- Versión de la distribución

Con dichas métricas se obtendrá el nivel de cumplimiento por punto de referencia

CIS previa y posteriormente a la ejecución del sistema automatizado de reforzamiento continuo de seguridad en sistemas Linux, con el objetivo de comparar los resultados y determinar la efectividad del sistema implementado.

Se utilizará un análisis cuantitativo de tipo comparativo, el cual permitirá contrastar los datos recopilados antes y después de la implementación del sistema automatizado, para examinar la mejora en la seguridad y la reducción de vulnerabilidades. Este análisis permitirá evaluar la efectividad del sistema automatizado.

CAPÍTULO II

MARCO TEÓRICO

2.1. Hardening de Seguridad

Vulnerabilidades

Las vulnerabilidades se refieren a debilidades en sistemas, aplicaciones o configuraciones que pueden ser explotadas por amenazas para comprometer la seguridad de un sistema. Las vulnerabilidades se encuentran priorizadas de acuerdo con el Sistema Común de Puntuación de Vulnerabilidad (CVSS). [9] Estas debilidades pueden incluir fallos de software, configuraciones incorrectas o falta de actualizaciones de seguridad, por lo cual existe siempre la posibilidad de que se produzcan nuevas vulnerabilidades en los sistemas. [10]

Amenazas

Una amenaza es cualquier entidad, proceso o evento que tiene el potencial de causar daño a un sistema de información. Las amenazas se encuentran en constante evolución, pueden ser nuevas y emergentes, entre las más conocidas se incluyen las de tipo virus, malware, ataques cibernéticos, errores humanos y

desastres naturales.[11]

Superficie de ataque

La superficie de ataque se refiere al conjunto de puntos de entrada o vulnerabilidades en un sistema que se encuentran expuestos y podrían ser explotados por amenazas mediante ataques de ciberseguridad. [7] Cuanto mayor sea la superficie de ataque, mayores serán las oportunidades para un atacante de comprometer la seguridad del sistema, por lo cual es importante reducir la superficie de ataque de los sistemas, elevando el nivel de dificultad para los atacantes. [9]

Marcos de referencia

Existen varios marcos de referencia de ciberseguridad que proporcionan pautas y mejores prácticas para fortalecer la seguridad de los sistemas. Estos marcos son utilizados por organizaciones para desarrollar estrategias de ciberseguridad efectivas.

Entre los tipos más conocidos se identifican el CIS - Critical Security Controls el cual ayuda a las organizaciones a mejorar sus estándares de seguridad; el ETSI - European Telecommunications Standards Institute el cual produce normas de telecomunicaciones utilizadas principalmente en Europa; el ISO/IEC 27000 - International Organization for Standardization / International Electrotechnical Commission que provee una serie de normas técnicas de seguridad de tecnologías de la información; y el NIST Cybersecurity Framework - National Institute of Standards and Technology diseñado con enforque para mantener la confidencialidad, integridad y disponibilidad de un sistema y su información. [8]

Para el presente proyecto se utilizará como marco de referencia de ciberseguridad el CIS - Critical Security Controls.

Cumplimiento normativo

El cumplimiento normativo implica la adhesión a regulaciones y estándares de seguridad establecidos por entidades reguladoras. El cumplimiento normativo es fundamental para garantizar que las organizaciones cumplan con requisitos legales y estándares de seguridad específicos. Los estándares de seguridad existentes ofrecen información sobre los controles, procesos, procedimientos, líneas base y directrices de seguridad recomendadas para el cumplimiento. [8]

2.2. Sistemas Linux

Los sistemas Linux son sistemas operativos basados en el núcleo o kernel Linux, los cuales se identifican por las siguientes características:

- **Flexibilidad y Configuración**: Linux es altamente flexible en cuanto a la configuración del sistema, lo que ha contribuido a su dominio en la lista de las 500 supercomputadoras principales. [10]

- **Enfoque General**: Linux se centra en desarrollar características de propósito general y no está limitado a una aplicación o uso específico. [10]

- **Eficiencia y Rendimiento**: En comparación con Windows, Linux tiende a ser más rápido y eficiente, con un uso de CPU más alto al ejecutar el mismo programa bajo condiciones de hardware similares. [11]

- **Confianza en Misiones Críticas**: Se confía en Linux incluso para aplicaciones cruciales en empresas, gobiernos y en misiones espaciales,

lo que demuestra su fiabilidad y seguridad.[12]

- **Tamaño y Complejidad**: El kernel de Linux tiene un número considerable de líneas de código, lo que indica su amplitud y sofisticación. [12]

- **Versatilidad en Hardware**: Linux es compatible con una amplia gama de hardware, desde supercomputadoras hasta dispositivos de IoT, lo que demuestra su flexibilidad y adaptabilidad. [13]

- **Seguridad**: Linux utiliza mecanismos de autoprotección, como el "Kernel Address Space Layout Randomization" (KASLR) y el "Kernel Page Table Isolation" (KPTI), para protegerse contra vulnerabilidades. [13]

- **Lenguaje de Programación y Modularidad**: El kernel de Linux está mayormente escrito en C, lo que lo hace rápido, pero con características de seguridad mínimas. Además, Linux utiliza módulos de kernel cargables, lo que permite extender su funcionalidad sin necesidad de reiniciar el sistema. [13]

- **Vulnerabilidades**: Aunque el número de vulnerabilidades descubiertas parece estar disminuyendo, sigue habiendo un número significativo de informes de CVE, y es posible que existan más vulnerabilidades no descubiertas y explotadas. [13]

- **Contenerización**: Mediante características del Kernel de Linux es posible soportar arquitecturas de microservicios con Contenedores. [14]

Para equipos servidores la distribución Linux más utilizada es Red Hat, debido a su alta adaptabilidad a entornos corporativos y capacidad de satisfacer las

demandas de infraestructuras complejas. Para equipos de usuario final la distribución Linux más utilizada es Ubuntu, conocida por brindar facilidades de uso se volvió popular en computadoras de escritorio y portátiles. [15]

2.3. Reforzamiento Continuo

La evaluación continua implica la revisión periódica de las configuraciones de seguridad de un sistema [5] para identificar y abordar vulnerabilidades y amenazas de manera proactiva. Esto contrasta con las evaluaciones puntuales que solo se realizan en momentos específicos. Permite verificar el nivel de cumplimiento de estándares de seguridad requeridos [4], evaluar técnicas de protección aplicadas [7] e identificar configuraciones que deben ser mejoradas [6].

El reforzamiento continuo ofrece ventajas clave, como la identificación temprana de problemas de seguridad con base a cumplimiento de estándares normativos, la adaptabilidad a las amenazas cambiantes, mejorar y mantener la postura de seguridad con el tiempo protegiendo los sistemas ante ciber amenazas [2]–[4]. Estos aportes contribuirán principalmente para minimizar la superficie de ataque ante actores maliciosos [1].

La evaluación continua es esencial en un entorno cibernético en constante evolución, donde las amenazas y vulnerabilidades cambian constantemente [4], [5]. Proporciona una estrategia efectiva para mantener la seguridad de los sistemas mediante la detección de incumplimientos de estándares de configuración, maximizando la protección de información que reside en los sistemas [2].

Las partes interesadas en la evaluación continua de la seguridad pueden incluir a los propietarios de sistemas, administradores de seguridad, profesionales de TI y

reguladores. Cada parte interesada desempeña un papel en garantizar que se mantenga la seguridad de los sistemas. [1]

CAPÍTULO III

PANORAMA TECNOLÓGICO EN PYMES Y SUS VULNERABILIDADES

3.1. Introducción a las tecnologías utilizadas en PYMES

Las pequeñas y medianas empresas (PYMES) se encuentran inmersas en un entorno empresarial cada vez más digitalizado, donde el uso estratégico de la tecnología ante el cambiante panorama digital es fundamental para su crecimiento y desarrollo. La infraestructura digital ha sido identificada como un importante impulsor de crecimiento financiero a largo plazo y de la capacidad de adaptación para las pequeñas y medianas empresas (PYMES).

Con base en el último reporte “The Future of Jobs Report” (World Economic Forum, 2023), bajo el cual se encuestó a 803 empresas en 27 industrias y 45 economías globales sobre las tendencias laborales, se afirma que las aplicaciones y plataformas digitales son las tecnologías más susceptibles para adoptar por las empresas, estimando que un 86% de ellas las incorporen en sus operaciones durante los próximos cinco años. [1].

En la actualidad, las PYMES mantienen una flexibilidad de tecnologías dentro de su infraestructura informática, a través de una combinación de sistemas operativos. De acuerdo con el reporte “Q4 2022 IT Trends for Small and Medium-Sized Enterprises (SMEs)” (JumpCloud, 2022), los administradores de TI esperan mantener dicha diversidad de dispositivos a medida que proyectan aumentos en el uso de dispositivos con sistemas operativos Windows (56.8%), macOS (40.2%) y Linux (35.3%). [12]

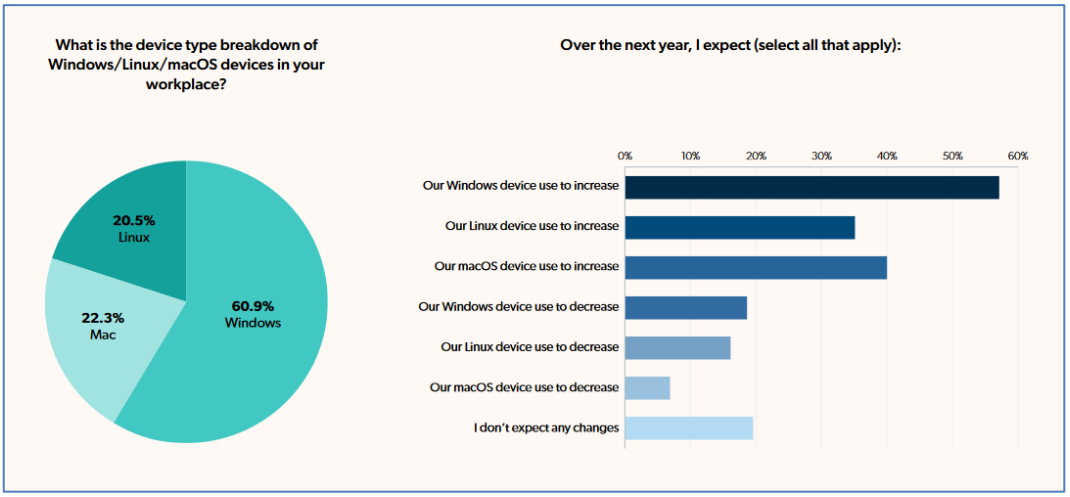

Ilustración 1: Panorama de sistemas operativos utilizados en PYMES

Fuente: Managing IT Amidst Rising Security Threats and Global Turbulence for Small to Medium-Sized Enterprises

Según las estadísticas de uso de sistemas operativos para implementación de servidores web (W3Techs, 2023), Linux es el sistema operativo fundamental para más del 81% de los sitios web publicados y en 2021, se estimaba que alrededor del 90% de las cargas de trabajo de la nube pública se ejecutaban en Linux.

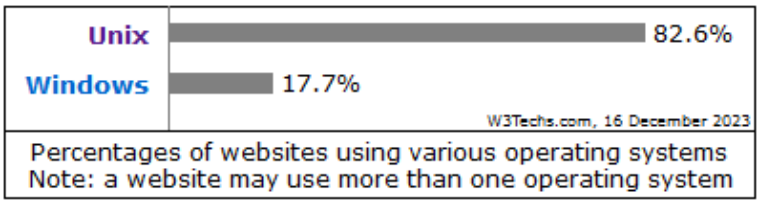

Ilustración 2: Distribución de sistemas operativos utilizados por sitios web

Fuente: https://w3techs.com/technologies/overview/operating_system

3.2. Vulnerabilidades en sistemas informáticos comunes en PYMES

De manera general, cada año se observa un incremento constante en el número de nuevas vulnerabilidades identificadas, demostrando un aumento continuo en los fallos de seguridad. De acuerdo con el reporte “Vulnerability and Threat Trends Report 2023” (Skybox, 2023), en el año 2022 se registró un récord por 25096 nuevas vulnerabilidades detectadas. Este incremento representa un aumento interanual del 25% en comparación con el año anterior. [13]

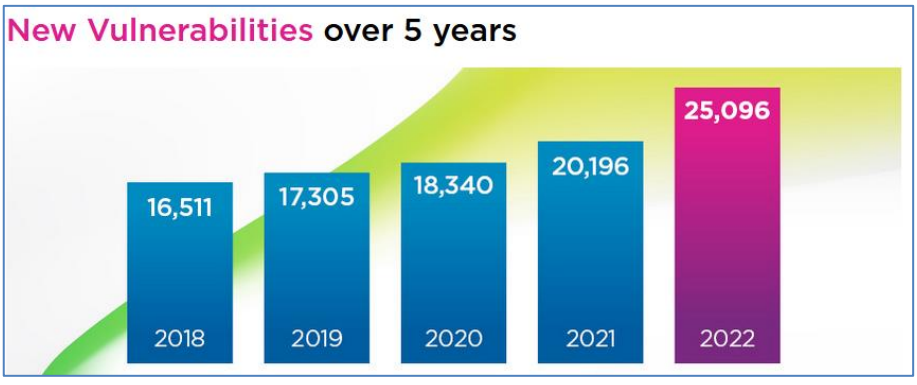

Ilustración 3: Tendencia anual de detección de nuevas vulnerabilidades

Fuente: Skybox – Vulnerability and Threat Trends Report 2023

Entre los principales productos afectados con el mayor porcentaje de vulnerabilidades reportadas en 2022 se encuentran los sistemas operativos Linux y Windows, utilizados ampliamente en servidores, revelando que los sistemas más

grandes y complejos suelen tener más vulnerabilidades. [13] Este indicador recalca la importancia de aplicar configuraciones y controles adecuados para proteger los servidores ante la gran cantidad de vulnerabilidades.

Ilustración 4: Top 10 productos con mayor volumen de vulnerabilidades

Fuente: Skybox – Vulnerability and Threat Trends Report 2023

Las PYMES enfrentan varios desafíos en la ciberseguridad, lo que las hace aún más vulnerables ante posibles ciberataques. Entre las principales debilidades que se presentan con mayor frecuencia se puede identificar las siguientes:

Recursos limitados

Las PYMES generalmente tienen presupuestos más reducidos y menos recursos para invertir en soluciones de seguridad empresarial en comparación

con las grandes empresas. Como resultado, es posible que carezcan de una infraestructura integral de ciberseguridad, herramientas y personal para defenderse contra amenazas cibernéticas sofisticadas. Además, sus recursos limitados significan que no pueden adquirir productos y equipos de alta gama y pueden verse obligadas a optar por artículos de menor presupuesto.

Tecnología desactualizada

Las PYMES a menudo confían en estrategias básicas de seguridad, como firewalls y software antivirus, debido a que las tecnologías de ciberseguridad más recientes pueden resultar complejas, costosas o requerir conocimientos especializados para su mantenimiento. Las opciones de precios y paquetes ofrecidas por los proveedores a menudo no son atractivas para las PYMES, lo que dificulta la adquisición y el mantenimiento de tecnología de seguridad.

Falta de experiencia

Las PYMES pueden carecer de equipos de TI o ciberseguridad dedicados. En su lugar, a menudo dependen de personal de TI general o incluso de contratistas externos que podrían carecer de conocimientos y experiencia especializada en la gestión de amenazas cibernéticas. Las PYMES a menudo subcontratan ciertos servicios o utilizan software de terceros que puede carecer de medidas de seguridad sólidas. Los ciberdelincuentes pueden aprovechar estas vulnerabilidades para acceder a los sistemas de las PYMES de manera indirecta.

Falta de conciencia

La ciberseguridad podría no ser una prioridad para algunas PYMES,

especialmente aquellas en industrias tradicionales donde la digitalización no es central en sus operaciones. Esta falta de conciencia puede llevar a descuidar prácticas y medidas básicas de ciberseguridad. Los ciberdelincuentes a menudo asumen que las PYMES tienen menos seguridad sólida, convirtiéndolas en objetivos fáciles. Por lo tanto, las PYMES pueden ser blanco simplemente porque los atacantes las perciben como vulnerables.

Capacitación inadecuada

El 40% de las PYMES afirman que la falta de personal de seguridad calificado es una barrera para mantener una postura de seguridad. Las brechas de conocimiento y experiencia significan que los empleados pueden no sentirse seguros ni competentes para identificar amenazas peligrosas como ataques de ingeniería social y phishing. La capacitación en ciberseguridad ayuda a fomentar una cultura de seguridad, convirtiéndola en una consideración diaria a largo plazo en lugar de ser motivo de pánico. Los empleados de las PYMES pueden no recibir una capacitación adecuada en ciberseguridad, lo que los hace más susceptibles a ataques de ingeniería social como el phishing.

Amenazas internas y errores humanos

Mientras que los profesionales de TI se enfocan en amenazas externas como hackers, el peligro puede estar más cerca de casa. Errores comunes como contraseñas fáciles de adivinar, la falta de autenticación de múltiples factores y la poca comprensión de controles de acceso pueden poner en riesgo a la organización.

3.3. Riesgos y amenazas de seguridad

Las PYMES están en riesgo de sufrir ataques cibernéticos, ya que son consideradas objetivos fáciles para los ciberdelincuentes. Entre los principales ataques que pueden causar daños significativos a las empresas se encuentran los siguientes:

Ataques de ransomware

Las PYMES pueden ser objeto de ataques de ransomware, en los cuales los ciberdelincuentes cifran los datos y solicitan un rescate para su liberación.

Según el informe “ENISA’s Threat Landscape Report” (ENISA, 2020), la distribución de ransomware fue la segunda amenaza cibernética más común, representando el 28% de todos los incidentes de seguridad registrados. [14]

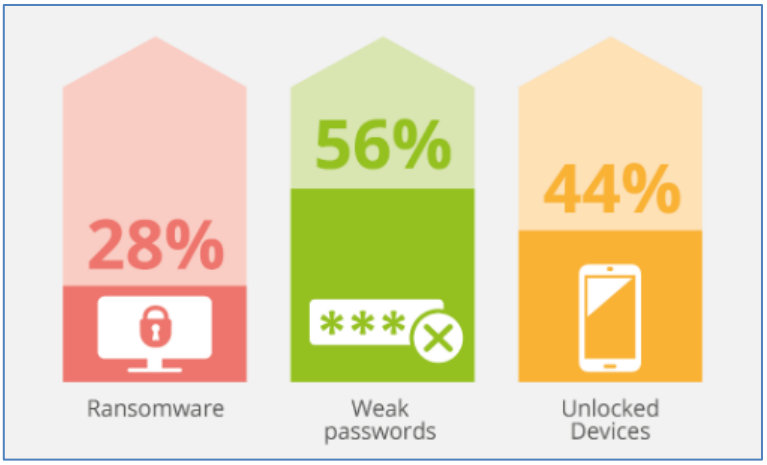

Ilustración 5: Panorama de ciberamenazas en PYMES

Fuente: ENISA – ENISA’s Threat Landscape Report 2020

Las PYMES afectadas suelen estar más inclinadas a pagar el rescate, ya que la pérdida de acceso a datos críticos podría ser devastadora para su actividad comercial.

Ataques de phishing

El phishing se ha convertido en el método preferido de los hackers para acceder a sistemas informáticos de individuos y empresas, ya que aprovecha

una vulnerabilidad que a menudo no puede ser protegida ni siquiera por los sistemas de seguridad informática más avanzados: la psicología humana y el error.

El phishing, el malware y los ataques basados en web son las causas raíz más comunes de incidentes de seguridad. [15]

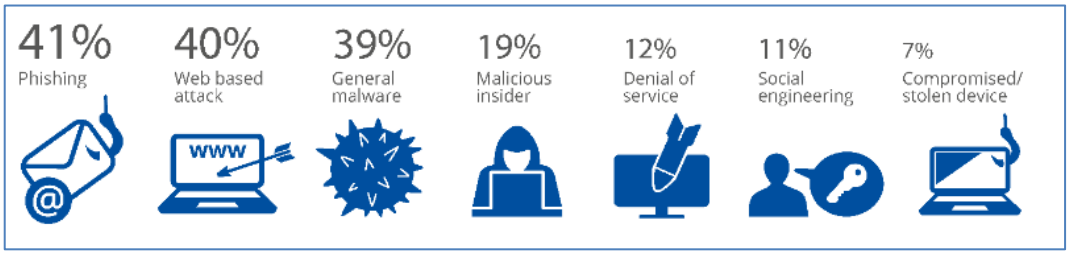

Ilustración 6: Distribución de ataques de ciberseguridad hacia PYMES en función de su origen

Fuente: ENISA Report - Cybersecurity for SMES Challenges and Recommendations

Ataques de malware

Estos ataques implican que los hackers implanten código malicioso en un ordenador o en la red de una empresa. Se pueden utilizar diversos medios para llevar a cabo esta acción, desde la conexión a dispositivos comprometidos hasta hacer clic en enlaces maliciosos en correos electrónicos no deseados o en sitios web.

Investigaciones de respuesta a incidentes han revelado que generalmente los dispositivos que han sido infectados carecen de software antivirus instalado con las bases actualizadas y tampoco tienen aplicado los últimos parches y actualizaciones de software. Para superar estos desafíos, las PYMES pueden tomar varias medidas proactivas para mejorar su postura de ciberseguridad,

tales como considerar implementar soluciones que les permitan administrar y controlar de forma centralizada cómo y cuándo se aplican los parches de software.

Esto también permitirá a la PYME tener visibilidad sobre qué dispositivos no se han parcheado correctamente y pueden necesitar atención adicional para remediarlos.

CAPÍTULO IV

DISEÑO DE PLAN DE IMPLEMENTACIÓN

4.1. Evaluación de mejores prácticas de seguridad

Con el propósito de robustecer la postura de seguridad de las de las pequeñas y medianas empresas (PYMES), existen diversos estándares de seguridad ampliamente aceptados en la industria, los cuales brindan lineamientos y guías para asegurar que los sistemas informáticos cumplan con esquemas reconocidos y sigan las directrices recomendadas para alcanzar un nivel óptimo de seguridad.

Para el presente proyecto, se empleará como marco de referencia en ciberseguridad el estándar CIS - Critical Security Controls, una elección respaldada por su enfoque riguroso y actualizado en la mitigación de riesgos y la promoción de prácticas de seguridad robustas.

CIS Benchmark, desarrollado por el Center for Internet Security (CIS), es un conjunto de directrices y mejores prácticas de seguridad diseñado específicamente para configuraciones de sistemas y aplicaciones con el objetivo de fortalecer la postura de seguridad. Este conjunto de normas se basa en la experiencia de expertos en ciberseguridad y abarca una amplia

gama de sistemas operativos y aplicaciones, proporcionando pautas detalladas para configuraciones seguras.

Aspecto	CIS Benchmark
Estandarización	Proporciona pautas y estándares específicos para la configuración de sistemas, redes y aplicaciones.
Mejores Prácticas	Ofrece un conjunto de mejores prácticas reconocidas en la industria para reforzar la seguridad de los sistemas.
Amplia Cobertura	Aborda una amplia gama de sistemas operativos y aplicaciones, incluyendo Linux, Windows, macOS y más.
Evaluación Continua	Facilita la evaluación continua y la aplicación de configuraciones seguras a lo largo del tiempo.
Comunidad Activa	Cuenta con una comunidad activa que actualiza regularmente las pautas para reflejar las amenazas y desafíos actuales.
Adaptabilidad	Puede adaptarse a diferentes entornos y requisitos de seguridad, proporcionando flexibilidad en la implementación.
Enfoque Integral	Ofrece pautas integrales que cubren aspectos clave de la seguridad, desde configuraciones básicas hasta medidas avanzadas.

Tabla 1: Fortalezas de CIS Benchmark

La elección de CIS Benchmark como marco de referencia para la evaluación

de mejores prácticas de seguridad en configuración de sistemas operativos basados en Linux se justifica por su enfoque exhaustivo y actualizado para abordar vulnerabilidades y configuraciones inseguras comunes.

Algunas de las directrices comunes que se cubren bajo el estándar CIS, para reducir la superficie de ataque y mejorar la resiliencia general del sistema frente a amenazas cibernéticas, son:

- Permisos de archivos y directorios: Configuraciones para garantizar que los permisos de archivos y directorios estén correctamente establecidos, limitando el acceso no autorizado.

- Configuración del firewall: Directrices para la configuración de reglas de firewall que controlan el tráfico de red y protegen contra amenazas externas.

- Configuración de servicios: Recomendaciones para la configuración segura de servicios del sistema operativo, desactivando servicios innecesarios y asegurando los esenciales.

- Configuración de red: Pautas para asegurar la configuración de red, incluyendo restricciones de acceso, filtrado de paquetes y otras medidas de seguridad.

- Políticas de contraseñas: Directrices para establecer políticas de contraseñas robustas, incluyendo requisitos de longitud, complejidad y rotación.

- Auditoría y registros del sistema: Configuración de auditoría y registros

para registrar eventos importantes y facilitar la detección de actividades maliciosas.

- Configuración de seguridad del kernel: Recomendaciones para configurar opciones de seguridad a nivel del kernel del sistema operativo.

- Actualizaciones del sistema: Pautas para gestionar las actualizaciones del sistema operativo, asegurando que se apliquen parches de seguridad de manera oportuna.

4.2. Implementación de Mejores Prácticas de Seguridad

Selección de la herramienta

Una vez definidas las directrices de control que se cubren bajo el estándar CIS Benchmark, la elección de la herramienta que realizará la evaluación y reforzamiento continuo de cumplimiento de seguridad es una decisión crítica que afectará directamente la efectividad y la eficiencia del proceso.

Durante nuestro proyecto hemos elegido la plataforma Foreman como sistema a utilizar para la ejecución continua de auditoría y reforzamiento automatizado del cumplimiento de la seguridad en sistemas Linux, debido a que ofrece un conjunto integral de herramientas para automatizar tareas relacionadas con la administración de sistemas.

En este contexto, la elección de Foreman se destaca como una decisión estratégica respaldada por diversas razones fundamentales:

- Código abierto: Esto permite una mayor visibilidad y contribuciones de

la comunidad de usuarios, fomentando la mejora continua y la adaptabilidad a diversos entornos.

- Integración sencilla: La herramienta debe integrarse fácilmente con el entorno existente asegurando una implementación sin complicaciones.

- Soporte para estándares de seguridad: Debe ser capaz de evaluar el cumplimiento con estándares reconocidos, específicamente CIS Benchmark, para garantizar una seguridad sólida y alineada con las mejores prácticas.

- Flexibilidad en la configuración: La herramienta debe permitir configuraciones flexibles para adaptarse a los requisitos específicos del entorno y las políticas de seguridad establecidas.

- Automatización y programación: Debe admitir la automatización de las evaluaciones de cumplimiento y reforzamiento, permitiendo programar escaneos regulares para mantener la seguridad de manera continua.

- Generación de informes: La generación de informes debe ser clara y comprensible, proporcionando resultados detallados y acciones correctivas sugeridas.

- Documentación: Deber contar con documentación detallada que explique su configuración, funcionamiento y mejores prácticas para aprovechar al máximo sus capacidades.

- Actualizaciones y soporte: La herramienta debe recibir actualizaciones periódicas para adaptarse a las evoluciones de las amenazas y contar

con un soporte técnico sólido para resolver posibles problemas.

Implementación de plataforma Foreman

El despliegue de Foreman implica una serie de pasos meticulosos, que van desde la instalación inicial hasta la configuración y la integración con Puppet para la aplicación efectiva de políticas de seguridad. Este proceso no solo establece una interfaz centralizada para la administración de sistemas, sino que también sirve como la base para la evaluación y el refuerzo continuo.

El proceso de instalación de Foreman implica varios pasos clave para asegurar una implementación exitosa:

1) **Verificar requisitos del sistema**: Validar de que el sistema cumple con los requisitos necesarios, incluyendo recursos de hardware y software.

Requisitos Mínimos	Con Puppet Server	Sin Puppet Server
Memoria RAM	4 GB	2 GB
Espacio en Disco	2 GB	1 GB

Tabla 2: Foreman - Requisitos de hardware

2) **Instalación de Foreman:** Descargar e instalar Foreman en el servidor designado. Esto puede implicar el uso de gestores de paquetes como apt o yum, dependiendo del sistema operativo.

3) **Configuración inicial:** Después de la instalación, se realiza una configuración inicial, definiendo aspectos como el nombre del host, la dirección IP y otros parámetros específicos del entorno.

4) **Configuración del repositorio**: Se configuran los repositorios necesarios

para acceder a las versiones adecuadas de Foreman y sus dependencias.

5) **Integración con Puppet**: Foreman se integra con Puppet, una herramienta de gestión de configuración, para facilitar la aplicación coherente de políticas de seguridad y configuraciones en los sistemas.

Este flujo de pasos proporciona una visión general del proceso de configuración de Foreman, estableciendo las bases para la implementación del sistema automatizado de reforzamiento continuo de la seguridad en sistemas Linux.

Configuración de evaluaciones y acciones correctivas

En el proceso de implementación del sistema automatizado para el reforzamiento continuo de la seguridad en sistemas Linux, Foreman desempeña un papel crucial en la gestión integral de los equipos del entorno.

Primero, los equipos con sistemas operativos Linux dentro del entorno PYMES son ingresados y registrados en Foreman, estableciendo un inventario centralizado.

Posteriormente, se establece la conexión con estos equipos mediante Puppet, una herramienta de gestión de configuración que permite definir y aplicar políticas de seguridad de manera consistente en toda la infraestructura.

La sincronización entre Foreman y Puppet asegura que las configuraciones y directrices definidas en Foreman se apliquen de manera efectiva en cada servidor Linux registrado. A través de plantillas y scripts específicos, se cargan y ejecutan las evaluaciones CIS Benchmark en cada equipo, permitiendo la

identificación automática de posibles desviaciones del estándar de seguridad.

Este sistema automatizado no solo identifica las posibles desviaciones de las configuraciones seguras recomendadas por el estándar CIS, sino que, a través de su integración con Puppet, puede aplicar correcciones automáticamente, garantizando que cualquier brecha de seguridad identificada se aborde de inmediato y se restablezca la integridad del sistema. Esta capacidad agrega un nivel adicional de robustez y eficacia a la gestión de la seguridad en entornos PYMES con sistemas informáticos basados en Linux.

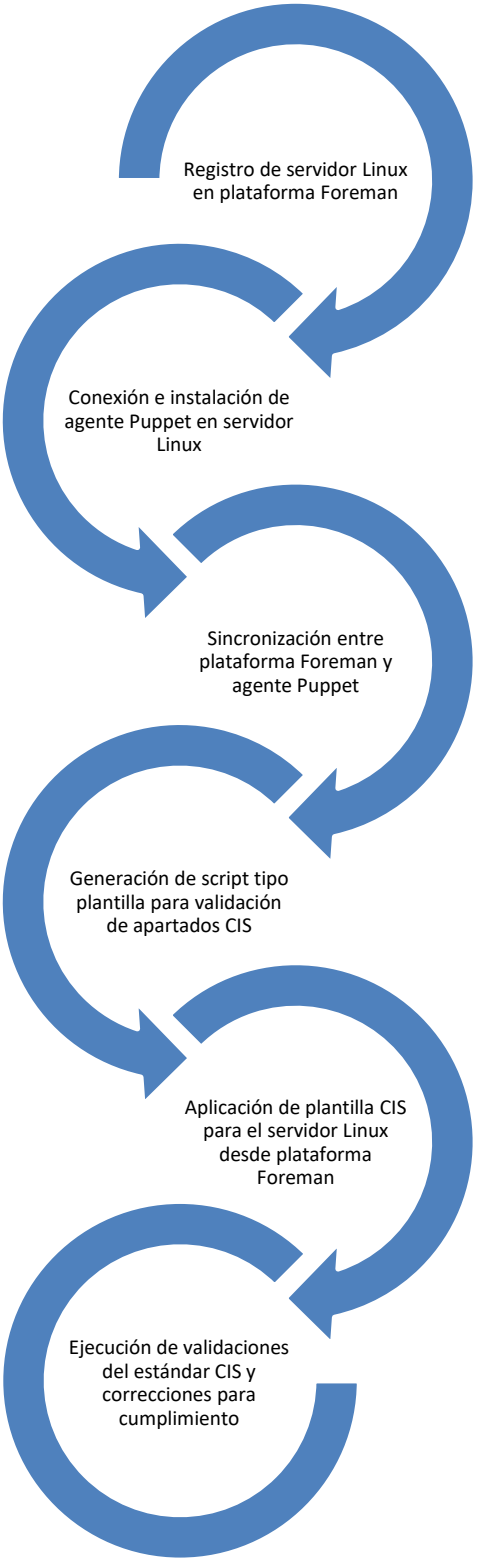

Ilustración 7: Flujo de configuración de evaluaciones con Foreman

4.3. Despliegue masivo de mejores prácticas de seguridad

Inventario de sistemas Linux

Para el despliegue masivo, se requiere la creación de un inventario completo de los sistemas basados en Linux que formarán parte del proceso de evaluación continua, asegurándose de cubrir todos los sistemas relevantes. Este inventario proporcionará una visión detallada de los activos críticos dentro de la organización PYME, facilitando la planificación y ejecución efectiva del despliegue masivo.

A continuación, se presenta una tabla detallada que describe los campos esenciales para un inventario de sistemas informáticos:

Campo	Descripción
ID Activo	Identificador único del sistema informático
Nombre del equipo	Nombre asignado al sistema dentro de la red
Dirección IP	Dirección IP asignada al sistema
Sistema operativo	Sistema operativo instalado en el equipo
Área responsable	Área encargada del mantenimiento y gestión
Función principal	Función principal del sistema (ej. Servidor web)
Estado	Estado actual del sistema (ej. Activo, Inactivo)

Tabla 3: Campos de interés para inventario de sistemas

Registro de sistemas Linux en plataforma Foreman

Una vez definido el inventario de sistemas, el paso final para garantizar el despliegue masivo del sistema automatizado de reforzamiento continuo de la seguridad en sistemas Linux consiste en el registro de dichos servidores en Foreman.

Al registrar los servidores del inventario de monitoreo, se establece la conexión administrativa con la plataforma Foreman, facilitando la evaluación y aplicación coherente de las mejores prácticas de seguridad definidas en la plantilla con base a los estándares de CIS Benchmark.

4.4. Ejecución continua de la evaluación y configuración de mejores

Evaluación continua de cumplimiento

Foreman permite programar que los escaneos de evaluación y reforzamiento continuo de la seguridad en sistemas Linux se ejecuten de manera automática en intervalos específicos, garantizando una evaluación continua de las configuraciones de seguridad.

Gestión de riesgos y remediaciones

Foreman, a través de su integración con Puppet, permite aplicar las correcciones y remediaciones de configuración de forma automática y simultánea durante el escaneo de evaluación, abordando de manera inmediata fallos de seguridad en el sistema monitoreado.

Generación de reportes

Los resultados de las ejecuciones se registran para documentar cambios, configuraciones y ajustes realizados durante el proceso. En caso de detectar desviaciones, es factible también activar alertas inmediatas para identificar una brecha de seguridad potencial y permitir una respuesta rápida.

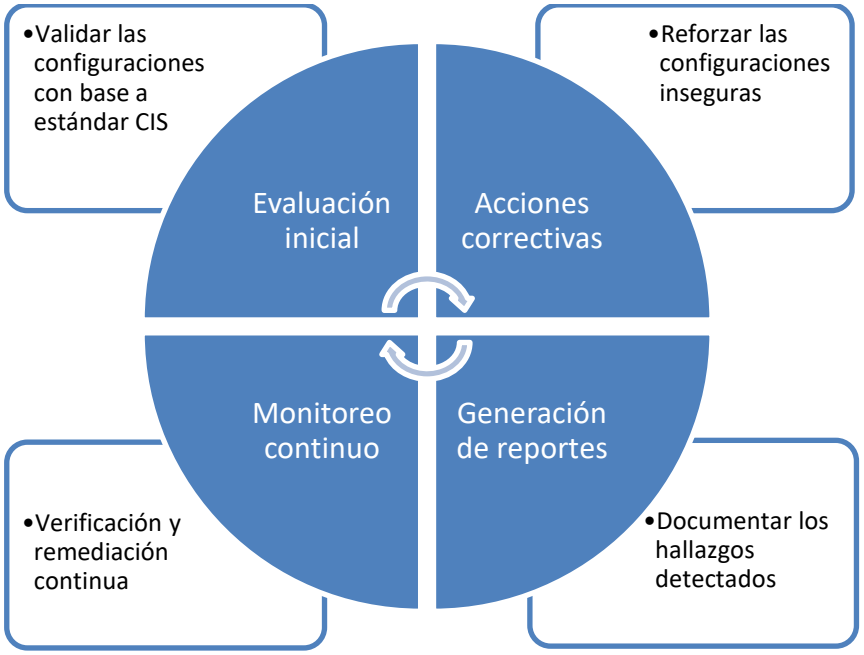

Ilustración 8: Ciclo de vida del sistema automatizado de reforzamiento continuo de la seguridad en sistemas Linux

CAPÍTULO V

IMPLEMENTACIÓN DEL PLAN

5.1. Implementación de prueba piloto

La prueba piloto se realiza sobre un ambiente controlado, el cual está compuesto por los siguientes equipos:

ID	Nombre	IP	SO	Función	Estado
1	foreman	192.168.1.200	AlmaLinux 8	Administración centralizada de configuraciones	Activo
2	web1	192.168.1.201	AlmaLinux 8	Servidor web	Activo
3	web2	192.168.1.202	AlmaLinux 8	Servidor web	Activo
4	db1	192.168.1.203	AlmaLinux 8	Base de datos	Activo
5	db2	192.168.1.204	AlmaLinux 8	Base de datos	Activo
6	nessus	192.168.1.205	AlmaLinux 8	Escáner de vulnerabilidades y cumplimiento	Activo
7	extranet	192.168.1.207	AlmaLinux 8	Servidor web	Activo
8	ftp	192.168.1.208	AlmaLinux 8	Servidor FTP	Activo

Tabla 4: Prueba piloto - Inventario de equipos

Para la instalación del software Foreman se sigue los siguientes pasos en el servidor Foreman:

1. Instalación de repositorio Puppet con el comando “dnf -y install https://yum.Puppet.com/Puppet7-release-el-8.noarch.rpm”

2. Instalación de repositorio Foreman con el comando “dnf -y install https://yum.theforeman.org/releases/3.9/el8/x86_64/foreman-release.rpm”
3. Habilitar módulo Foreman con el comando “dnf -y module enable foreman:el8”
4. Descargar instalador con el comando “dnf -y install foreman-installer”
5. Ejecutar instalador con el comando “foreman-installer”
6. Al finalizar la instalación se muestra en pantalla las credenciales necesarias para acceder al software Foreman
7. Luego configurar el servidor Puppet mediante el comando “Puppet agent –test”

Para la primera parte de la prueba piloto se lleva a cabo en el servidor web2, el cual tiene un sistema operativo Linux, AlmaLinux 8, y la política de cumplimiento que se usará es CIS para AlmaLinux 8 nivel 1.

El primer paso, esencial para el inicio de la prueba piloto, implica una revisión inicial del cumplimiento de la normativa CIS para AlmaLinux 8 nivel 1 en el servidor web2, esta se realiza mediante la herramienta Nessus Professional con el tipo de escaneo Policy Compliance Auditing.

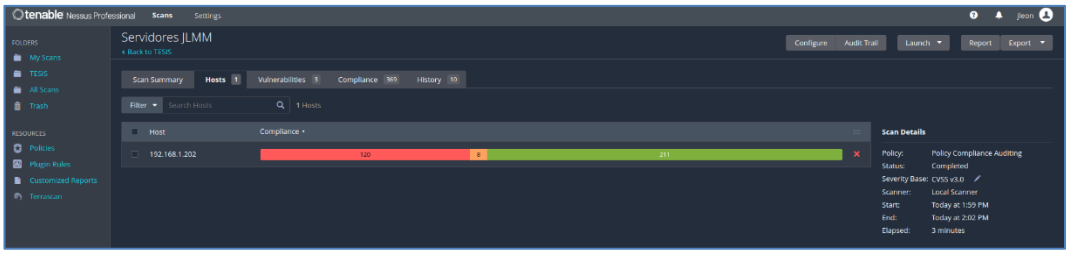

Ilustración 9: Prueba piloto – Evaluación inicial de cumplimiento

Como se observa en la imagen de un total de 339 puntos de revisión se incumplen 120 (en rojo), este escaneo dura aproximadamente 3 minutos.

El siguiente paso, para facilitar el control de muchos equipos que cumplan un rol similar se procede con la creación de Host Group “Servidores Web”, este nos permitirá aplicar la misma configuración a todos los miembros de forma grupal evitando la necesidad de aplicarla uno por uno.

Registrar los servidores en Foreman constituye un proceso clave para la centralización de configuraciones y facilita el despliegue masivo de las mismas, por lo que registrar el servidor web2 es el tercer paso y para esto es necesario generar el comando de registro desde Foreman. La información necesaria se muestra en la siguiente imagen.

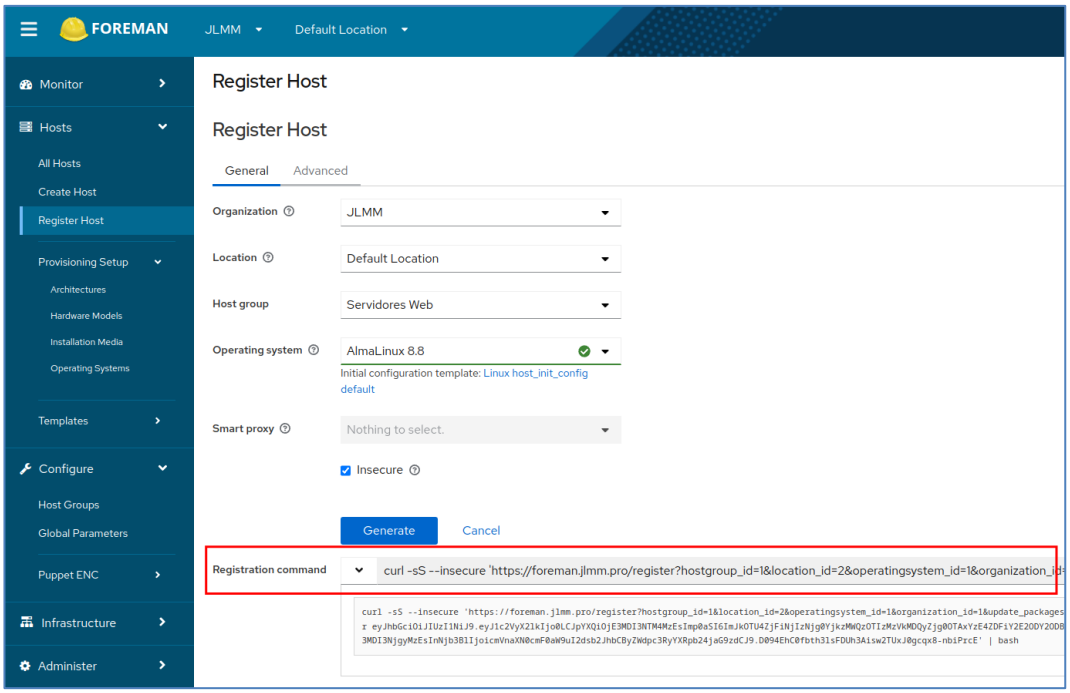

Ilustración 10: Prueba piloto - Generación de comando de registro

El comando de registro se ejecuta en el servidor web2 como usuario root y tarda unos minutos en culminar.

```
[root@web2 ~]# curl -sS --insecure 'https://foreman.jlmm.pro/register?hostgroup_id=1&location_id=2&oper
1c2VyX2lkIjo0LCJpYXQiOjE3MDI3NTM4MzEsImp0aSI6ImJkOTU4ZjFiNjIzNjg0YjkzMWQzOTIzMzVkMDQyZjg0OTAxYzE4ZDFiY2
4jaG9zdCJ9.D094EhC0fbth3lsFDUh3Aisw2TUxJ0gcqx8-nbiPrcE' | bash
#
# Running registration
#
# Running [web2.jlmm.pro] host initial configuration
```

Ilustración 11: Prueba piloto - Registro de servidor

Para validar que el registro del servidor en Foreman se haya realizado de forma exitosa se usa el comando “Puppet agent -t”, como resultado se obtiene un mensaje indicando que el catálogo se aplicó correctamente.

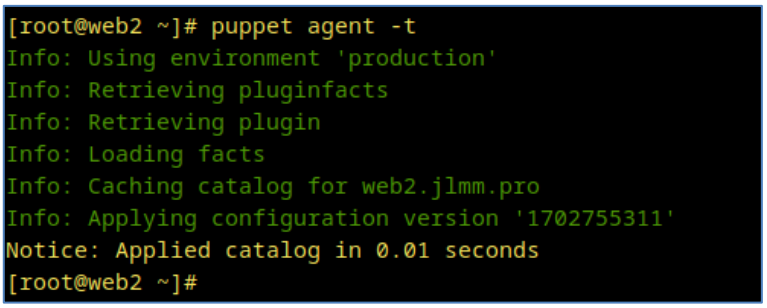

Ilustración 12: Prueba piloto - Validación de registro

Foreman para gestionar configuraciones se ayuda de Puppet, tiene embebido un servidor Puppet, este puede hacer uso del repositorio público Forge para obtener plantillas de configuraciones hechas por empresas o miembros de la comunidad que utiliza Puppet.

Desde Forge descargamos e instalamos en el Puppet Server el módulo tomkrieger-cis_security_hardening, por ser el más completo respecto a configuraciones de cumplimiento de CIS, gratis y tener actualizaciones recientes, a través del comando “Puppet module install tomkrieger-cis_security_hardening --version 0.9.1”

Adicionalmente se descarga e instala el módulo treydock-yum_cron a través del comando “Puppet module install treydock-yum_cron --version 7.1.0” para gestionar las actualizaciones automáticas de los equipos Linux, puesto que tener el equipo actualizado es uno de los puntos de revisión de CIS AlmaLinux8 nivel 1.

Luego de importar los módulos Puppet en Foreman y para facilitar la gestión de configuraciones se crea el grupo de configuración “CIS_AlmaLinux8” con

los módulos antes mencionados.

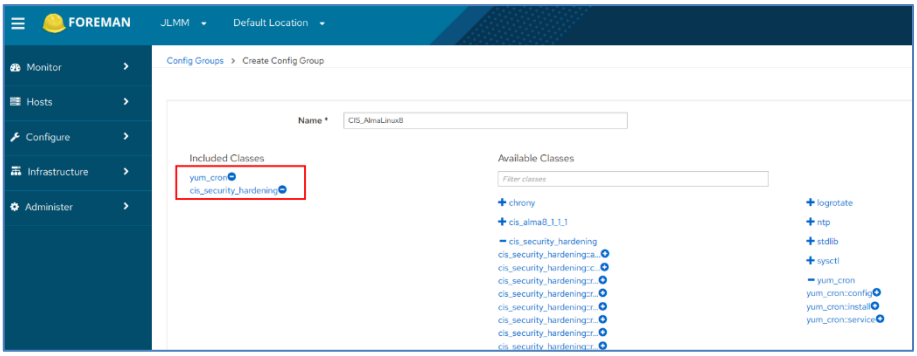

Ilustración 13: Prueba piloto - Creación de grupo de configuración

Para desplegar el grupo de configuración “CIS_AlmaLinux8” se procede a editar el Host e ir al apartado de Puppet ENC.

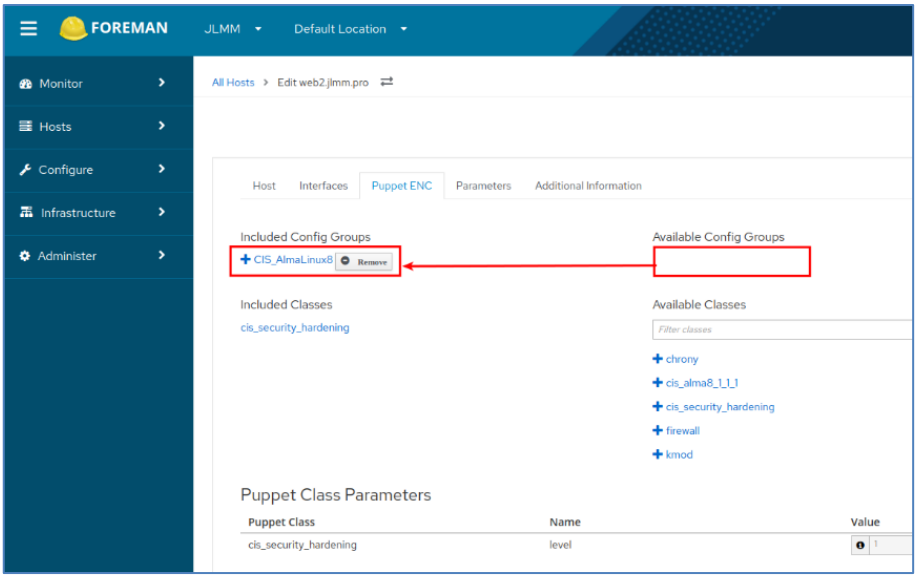

Ilustración 14: Prueba piloto - Aplicación de configuración

Posteriormente para evitar esperar la sincronización entre el agente Puppet y el servidor Puppet se procede a forzar la aplicación de la configuración mencionada en el paso anterior.

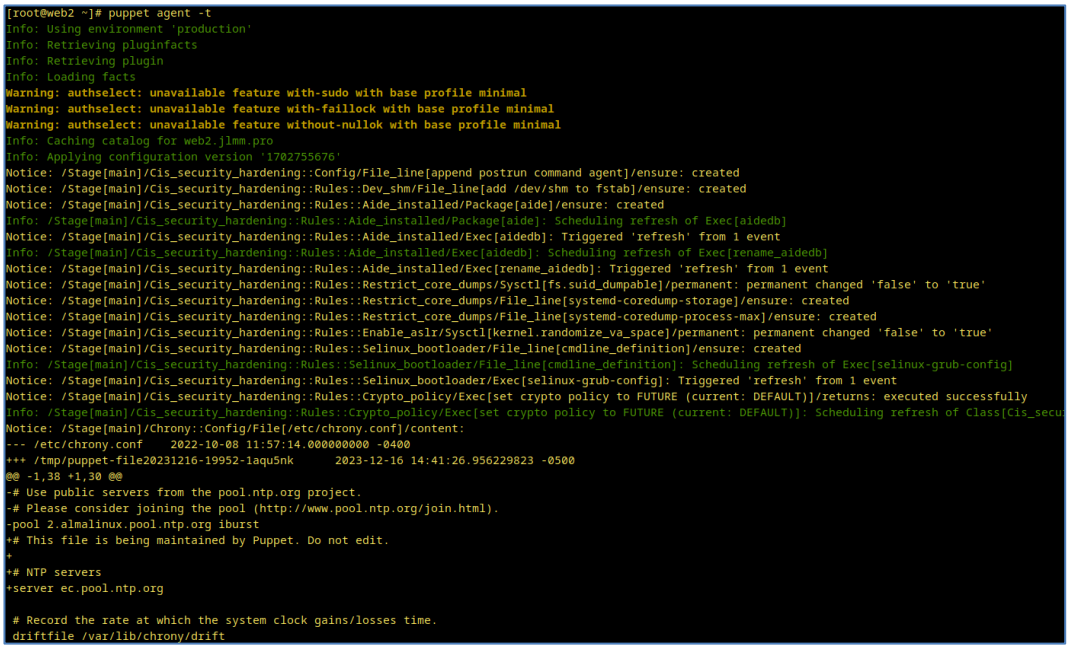

Ilustración 15: Prueba piloto – Aplicación forzada de configuración

Para finalizar la primera parte de la prueba, mediante la herramienta de escaneo de vulnerabilidades y cumplimiento Nessus se realiza una revisión exhaustiva del cumplimiento de la normativa CIS para AlmaLinux 8 nivel 1 en el servidor web2. Este análisis final permite confirmar que todas las configuraciones y medidas de seguridad han sido implementadas de manera efectiva, cumpliendo con los estándares establecidos y asegurando la integridad del servidor web2 en términos de seguridad.

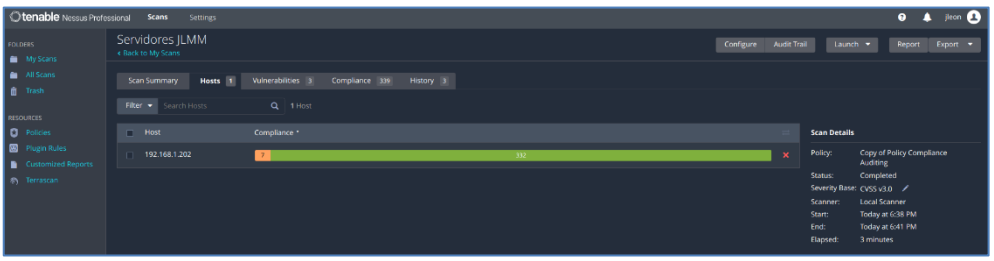

Ilustración 16: Prueba piloto – Evaluación de cumplimiento final

Como se evidencia en la imagen anterior se tiene 339 puntos de revisión y ninguno marcado como incumplido (en rojo).

Para comprobar la aplicación continua de las configuraciones que permiten el cumplimiento del CIS AlmaLinux8 nivel 1 se modificará el archivo de configuración del servidor SSH de web2 añadiendo el usuario ficticio “cuenta-hacker” entre las cuentas permitidas.

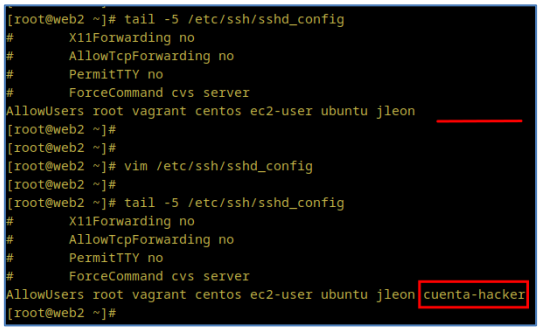

Ilustración 17: Prueba piloto – Cambio manual de configuración SSH

Luego de unos minutos el agente Puppet al identificar que la configuración del servicio ssh no está como indica Foreman se procede con el ajuste, retirando la cuenta ficticia.

Ilustración 18: Prueba piloto – Aplicación automática de corrección

En logs del servidor web2 es visible que se toma acción sobre el parámetro modificado previamente.

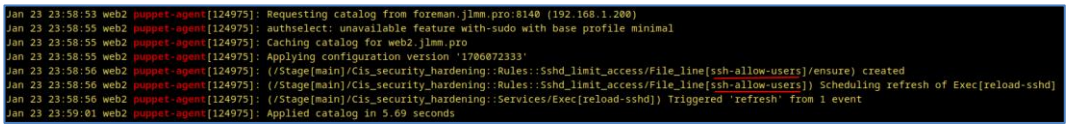

Ilustración 19: Prueba piloto – Logs de la corrección automática

Una vez validado el funcionamiento para 1 servidor (web2) se procede a repetir el proceso para los demás equipos para culminar la prueba piloto, pasando de 120 puntos de revisión incumplidos a 0 en pocos minutos.

Ilustración 20: Prueba piloto – Evaluación inicial de cumplimiento en despliegue masivo

Ilustración 21: Prueba piloto - Evaluación final de cumplimiento en despliegue masivo

5.2. Revisión de resultados

Dado que el número de incumplimientos de los puntos de revisión del CIS Benchmark AlmaLinux 8 nivel 1 se reduce a 0 al aplicar las configuraciones de endurecimiento en los servidores de la prueba piloto desde Foreman y luego de haber probado que las modificaciones que se realizan manualmente sobre los servidores registrados en Foreman son sobrescritas por las configuraciones aplicadas con Puppet, se concluye que el resultado está acorde a lo esperado, es decir, con Foreman logramos aplicar y mantener en el tiempo configuraciones de endurecimiento que permiten cumplir los requerimientos por CIS.

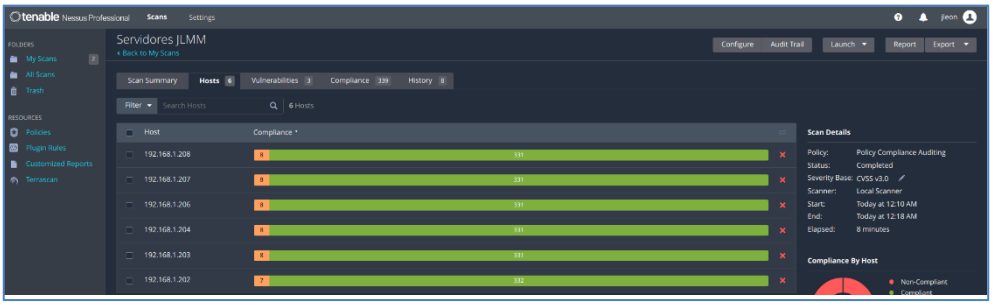

Ilustración 22: Prueba piloto - Evaluación continua de cumplimiento en despliegue masivo

CONCLUSIONES

1) Se ha logrado realizar un análisis del panorama tecnológico en PYMES, identificando vulnerabilidades, riesgos y amenazas de seguridad asociados a las tecnologías utilizadas. Este análisis proporciona una comprensión profunda de la estrategia de ciberseguridad y sienta las bases para enfoques más efectivos en la protección de sistemas.

2) La investigación ha culminado en la creación de un plan de implementación detallado que aborda la evaluación del estado de configuración de sistemas Linux. Este plan incorpora recomendaciones específicas basadas en estándares de seguridad reconocidos, lo que brinda a las PYMES una guía práctica para fortalecer sus posturas de seguridad.

3) Como resultado directo de la investigación, se ha implementado con éxito un sistema automatizado destinado a la evaluación y reforzamiento continuo de las mejores prácticas de configuración a nivel de seguridad en sistemas Linux en entornos PYMES. Este sistema proporciona una solución eficiente y escalable para mantener la seguridad de los sistemas de manera proactiva.

RECOMENDACIONES

1) Se recomienda realizar revisiones periódicas de las políticas de seguridad y de las evaluaciones CIS para asegurar que estén alineadas con las últimas tendencias latentes de amenazas cibernéticas y vulnerabilidades que afecten principalmente a los entornos PYMES.

2) Proporcionar capacitación continua al personal encargado de la administración y configuración de sistemas, garantizando que estén al tanto de las mejores prácticas de seguridad y del uso eficiente de las herramientas implementadas.

3) Implementar sistemas de monitorización activa para detectar posibles desviaciones de la configuración segura en tiempo real, permitiendo una respuesta inmediata ante cualquier anomalía detectada que pudiera ser indicador de compromiso del sistema.

4) Explorar oportunidades para integrar otros sistemas operativos, nuevas tecnologías y/o herramientas de seguridad en el proceso de evaluación y reforzamiento del sistema automatizado, manteniéndolo actualizado frente a los desafíos emergentes en el panorama de ciberseguridad.

REFERECIA BIBLIOGRÁFICA

[1] F. E. Mundial, “The future of jobs report,” in *World Economic Forum*, 2023.
[2] Z. McLennan Marsh, “The Global Risks Report 2023 18th Edition,” World Economic Forum Cologny, Switzerland, 2023.
[3] O. Kinger Bharti, “The Linux Threat Landscape Report,” *Trend Micro*, 2023.
[4] M. Jogi, “Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance,” *University of Tartu, Tartu*, 2017.
[5] A. Bicaku, M. Zsilak, P. Theiler, M. Tauber, and J. Delsing, “Security Standard Compliance Verification in System of Systems,” *IEEE Systems Journal*, vol. 16, no. 2, pp. 2195–2205, 2022, doi: 10.1109/JSYST.2021.3064196.
[6] J. F. Carías, S. Arrizabalaga, L. Labaka, and J. Hernantes, “Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs,” *IEEE Access*, vol. 9, pp. 80741–80762, 2021, doi: 10.1109/ACCESS.2021.3085530.
[7] J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, “Systematic Approach to Cyber Resilience Operationalization in SMEs,” *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.
[8] C. Wright, C. Cowan, J. Morris, S. Smalley, and G. Kroah-Hartman, “Linux security module framework,” in *Ottawa Linux Symposium*, 2002, pp. 6–16.
[9] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, “A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow,” *IEEE Access*, vol. 6, pp. 8599–8609, 2018, doi: 10.1109/ACCESS.2018.2805690.
[10] F. Djebbar and K. Nordström, “A Comparative Analysis of Industrial Cybersecurity Standards,” *IEEE Access*, vol. 11, pp. 85315–85332, 2023, doi: 10.1109/ACCESS.2023.3303205.
[11] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, “A Review of Security Standards and Frameworks for IoT-Based Smart Environments,” *IEEE Access*, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
[12] JumpCloud, “Q4 2022 IT Trends for Small and Medium-Sized Enterprises (SMEs),” in *JumpCloud*, 2022.
[13] Skybox, “Vulnerability and Threat Trends Report 2023,” in *Skybox*, 2023.
[14] ENISA, “ENISA’s Threat Landscape reports,” in *ENISA*, 2020.
[15] ENISA, “ENISA Report - Cybersecurity for SMES Challenges and Recommendations,” in *ENISA*, 2021.

[9] M. Jogi, “Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance,” University of Tartu, Tartu, 2017.
[10] A. Bicaku, M. Zsilak, P. Theiler, M. Tauber, and J. Delsing, “Security Standard Compliance Verification in System of Systems,” IEEE Systems Journal, vol. 16, no. 2, pp. 2195–2205, 2022, doi: 10.1109/JSYST.2021.3064196.
[11] J. F. Carías, S. Arrizabalaga, L. Labaka, and J. Hernantes, “Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs,” IEEE Access, vol. 9, pp. 80741–80762, 2021, doi: 10.1109/ACCESS.2021.3085530.
[12] J. F. Carías, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, “Systematic Approach to Cyber Resilience Operationalization in SMEs,” IEEE Access, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.
[13] C. Wright, C. Cowan, J. Morris, S. Smalley, and G. Kroah-Hartman, “Linux security module framework,” in Ottawa Linux Symposium, 2002, pp. 6–16.
[14] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, “A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow,”

IEEE Access, vol. 6, pp. 8599–8609, 2018, doi: 10.1109/ACCESS.2018.2805690.
[15] F. Djebbar and K. Nordström, “A Comparative Analysis of Industrial Cybersecurity Standards,” IEEE Access, vol. 11, pp. 85315–85332, 2023, doi: 10.1109/ACCESS.2023.3303205.
[16] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, “A Review of Security Standards and Frameworks for IoT-Based Smart Environments,” IEEE Access, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
[17] E. van der Kouwe, G. Heiser, D. Andriesse, H. Bos, and C. Giuffrida, “SoK: Benchmarking Flaws in Systems Security,” in 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019, pp. 310–325. doi: 10.1109/EuroSP.2019.00031.
[18] D. B. de Oliveira, D. Casini, and T. Cucinotta, “Operating System Noise in the Linux Kernel,” IEEE Transactions on Computers, vol. 72, no. 1, pp. 196–207, 2023, doi: 10.1109/TC.2022.3187351.
[19] S. Zhong, W. Ren, T. Zhu, Y. Ren, and K.-K. R. Choo, “Performance and Security Evaluations of Identity- and Pairing-Based Digital Signature Algorithms on Windows, Android, and Linux Platforms: Revisiting the Algorithms of Cha and Cheon, Hess, Barreto, Libert, Mccullagh and Quisquater, and Paterson and Schuldt,” IEEE Access, vol. 6, pp. 37850–37857, 2018, doi: 10.1109/ACCESS.2018.2853703.
[20] I. Allende, N. M. Guire, J. Perez-Cerrolaza, L. G. Monsalve, J. Petersohn, and R. Obermaisser, “Statistical Test Coverage for Linux-Based Next-Generation Autonomous Safety-Related Systems,” IEEE Access, vol. 9, pp. 106065–106078, 2021, doi: 10.1109/ACCESS.2021.3100125.
[21] C. E. Staniloiu, A. Militaru, R. Nitu, and R. Deaconescu, “Safer Linux Kernel Modules Using the D Programming Language,” IEEE Access, vol. 10, pp. 134502–134511, 2022, doi: 10.1109/ACCESS.2022.3229461.
[22] S. Sultan, I. Ahmad, and T. Dimitriou, “Container Security: Issues, Challenges, and the Road Ahead,” IEEE Access, vol. 7, pp. 52976–52996, 2019, doi: 10.1109/ACCESS.2019.2911732.
[23] S.-J. Jung and K. Sung, “Trend analysis and Classification of Linux distributions,” Journal of Digital Contents Society, vol. 18, no. 2, pp. 357–363, 2017.