Universidad de Buenos Aires
Facultades de Ciencias Económicas
Ciencias Exactas y Naturales e Ingeniería

MAESTRÍA EN SEGURIDAD INFORMÁTICA

TESIS DE MAESTRÍA

TEMA

HARDENING DE SERVIDORES

TÍTULO

DESARROLLO DE UN SISTEMA PARA FACILITAR Y AGILIZAR EL PROCESO DE HARDENING DE SERVIDORES LINUX

AUTOR: FABRICIO GABRIEL TORRICO BARAHONA

DIRECTOR DE TESIS: DR. PEDRO HECHT

2023

COHORTE 2020

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Fabricio Gabriel Torrico Barahona
CI: 6180245 LP, BOLIVIA

RESUMEN

El presente trabajo es desarrollado bajo una metodología exploratoria y descriptiva, tomando un enfoque mixto que parte de una investigación de herramientas, guías técnicas, estándares y soluciones que apoyan en el proceso de hardening de servidores y finaliza con un enfoque experimental que plantea el desarrollo de un sistema web que centraliza, facilita y agiliza el proceso de hardening de servidores Linux, incrementando la seguridad en las configuraciones en un promedio de 34% aplicando todas las funcionalidades disponibles en el sistema.

Palabras clave: Linux, open source, servicio, servidor, sistema operativo.

ÍNDICE

BIBLIOGRAFÍA

BLIOGRAFÍA GENERAL

ÍNDICE DE FIGURAS

AGRADECIMIENTOS

Sin lugar a dudas hay personas que siempre me acompañan y donde quiera estén siempre guían mis pasos ya sea física o espiritualmente. Quiero agradecer a mis queridos papás Walter, Alcira, Juan y Lidia, que seguramente se preocuparon por mi bienestar desde que nací, así como a mi novia Mischell y a todos mis familiares quienes me acompañaron y enseñaron tanto de una u otra manera. Sin embargo; este trabajo está totalmente dedicado a mis amados papás, a mi hermanita y a Dios, sin temor a equivocarme puedo decir que ellos son los principales artífices y sembradores de todo el éxito que vengo cosechando en mis 28 años. Mami, Papi, Gabi, gracias por todo el amor que me dan, son perfectos en todo sentido, los amo infinitamente.

.

CUERPO INTRODUCTORIO

I. INTRODUCCIÓN

Por los datos disponibles en Siteefy[1], a enero de 2023 existían a nivel mundial 1.132.268.801 sitios web, de los cuales 202.900.724 estaban realmente activos y se estima que aproximadamente cada minuto se crean 175 sitios web, lo que genera alrededor de 252.000 nuevos sitios web al día. Estos datos son simplemente un reflejo de la constante necesidad de exponer nuevos servicios; lamentablemente, la falta de personal especializado en seguridad en empresas pequeñas e incluso medianas, genera que el personal de sistemas ponga en producción servidores y servicios con configuraciones por defecto, que en consecuencia exponen brechas de seguridad fáciles de explotar. Así lo confirma el Centro de Recursos de Robo de Identidad[2], que determinó que la mala configuración de seguridad es muy común e informó que las configuraciones incorrectas están detrás de un tercio de las violaciones de datos informadas. Siempre es probable que ocurran errores costosos en las configuraciones cuando la seguridad se gestiona manualmente, además de que los productos tecnológicos por lo general están destinados a una amplia variedad de audiencias por lo que priorizan la usabilidad, haciendo que las configuraciones de seguridad restrictivas generalmente no estén habilitadas de manera predeterminada, lo que genera que muchos productos de sean vulnerables tras su implementación.

Si bien el problema está claramente identificado, es una realidad que el proceso de hardening es una tarea complicada, ardua y que demanda mucho tiempo, incluso a administradores de sistemas experimentados; saber cuál es el conjunto razonable de configuraciones de seguridad para distintos productos en sin duda una tarea complicada.

[1] https://siteefy.com/how-many-websites-are-there/#:~:text=Chapter%205-,How%20Many%20Websites%20Are%20Created%20Every%20Day%3F,up%20with%20a%20rough%20estimation.

[2] https://www.idtheftcenter.org/

Afortunadamente, existen organizaciones que publican guías de hardenización y estándares que permiten homogeneizar el proceso; que si bien son de gran ayuda, por lo generan son elementos que requieren su aplicación de manera aislada y con cierta expertiz, por lo que de cualquier modo requiere tiempo y dedicación.

El presente trabajo pretende recopilar información de fuentes públicas y proponer un sistema que facilite y agilice el proceso de hardening de servidores.

II. OBJETIVOS

La presente tesis contempla los siguientes objetivos.

II a. OBJETIVO GENERAL

Desarrollar un sistema para facilitar y agilizar el proceso de *hardening* de servidores Linux.

II b. OBJETIVOS ESPECÍFICOS

Los objetivos específicos son:

- Investigar documentos elaborados por organizaciones y expertos en la materia, que detallen las mejores prácticas de la industria y configuraciones seguras en servidores Linux.
- Investigar herramientas que ayuden a realizar el *hardening* de servidores Linux.
- Analizar, diseñar y desarrollar un sistema.
- Probar el sistema desarrollado y medir cuantitativamente las mejoras de seguridad producidas tras su uso.

III. ALCANCES

Los alcances de la tesis son los siguientes:

- Se analizarán documentos disponibles de manera libre y gratuita.
- Se analizarán herramientas gratuitas o de uso libre por tiempo limitado.
- El desarrollo del sistema estará enfocado en distribuciones Ubuntu Linux.

- El sistema implementará módulos de *hardening* de servicios web (Servidor Apache) y base de datos (MySQL o MariaDB) únicamente si durante la investigación se evidencia documentación confiable y avalada por organizaciones reconocidas relacionada con la temática de estudio.

IV. HIPÓTESIS

El sistema desarrollado mejora los niveles de seguridad de los servidores en los que se ejecuta.

V. METODOLOGÍA

El trabajo plantea una metodología exploratoria y descriptiva, tomando un enfoque mixto, donde el método de recolección y análisis de datos sigue un enfoque experimental.

CUERPO PRINCIPAL

1. ¿QUÉ ES HARDENING?

Antes de empezar a investigar guías o herramientas que permitan realizar la fortificación de sistemas, se desarrolla un breve párrafo que permita entender a qué hace referencia el término "*hardening"*.

Si bien la traducción literal al español es "endurecimiento", a lo largo del presente documento se utilizará el término en inglés. Se tienen diversas definiciones y de [1], [2], [3], [4], [5], [6], [7] y [8] se puede concluir que el *hardening* es un conjunto de medidas que se toman para reducir la superficie de ataque, los riesgos y vulnerabilidades asociados a elementos informáticos, a los que se está más propenso cuantas más funciones desempeña. Tomando como base la defensa en profundidad, se puede aplicar *hardening* en diferentes niveles; por ejemplo con la concientización del personal, aplicando medidas de seguridad física, en el perímetro, en la red interna, en el servidor, en las aplicaciones e inclusive en la información; si bien el presente trabajo se enfoca principalmente en medidas de *hardening* a nivel de servidor y aplicaciones, en un entorno empresarial se recomienda fortificar todos los niveles y no enfocarse únicamente en una capa.

A nivel de servidor y aplicaciones, el objetivo es modificar las configuraciones por defecto (que por lo general están orientados a la facilidad de uso y despliegue, olvidando la seguridad) y eliminar elementos innecesarios, buscando un equilibrio entre protección y usabilidad, haciendo notar que un sistema cerrado al mundo es muy seguro pero poco útil.

2. ORGANIZACIONES, ESTÁNDARES Y GUÍAS DE HARDENING

Existen diversas organizaciones, comunidades y entidades gubernamentales que publican guías o lineamientos para el proceso de hardenización. Se analiza a continuación las más relevantes y reconocidas mundialmente.

2.1. CIS - Center for Internet Security

CIS - Center for Internet Security, Inc. [9] es una organización independiente sin fines de lucro impulsada por la comunidad, fundada en agosto del 2000 y que lidera una comunidad global de profesionales de TI que tienen el objetivo de evolucionar continuamente diversos estándares y proporcionar productos y servicios para brindar protección de manera proactiva contra las amenazas emergentes. La siguiente imagen muestra las diversas soluciones que desarrolla CIS.

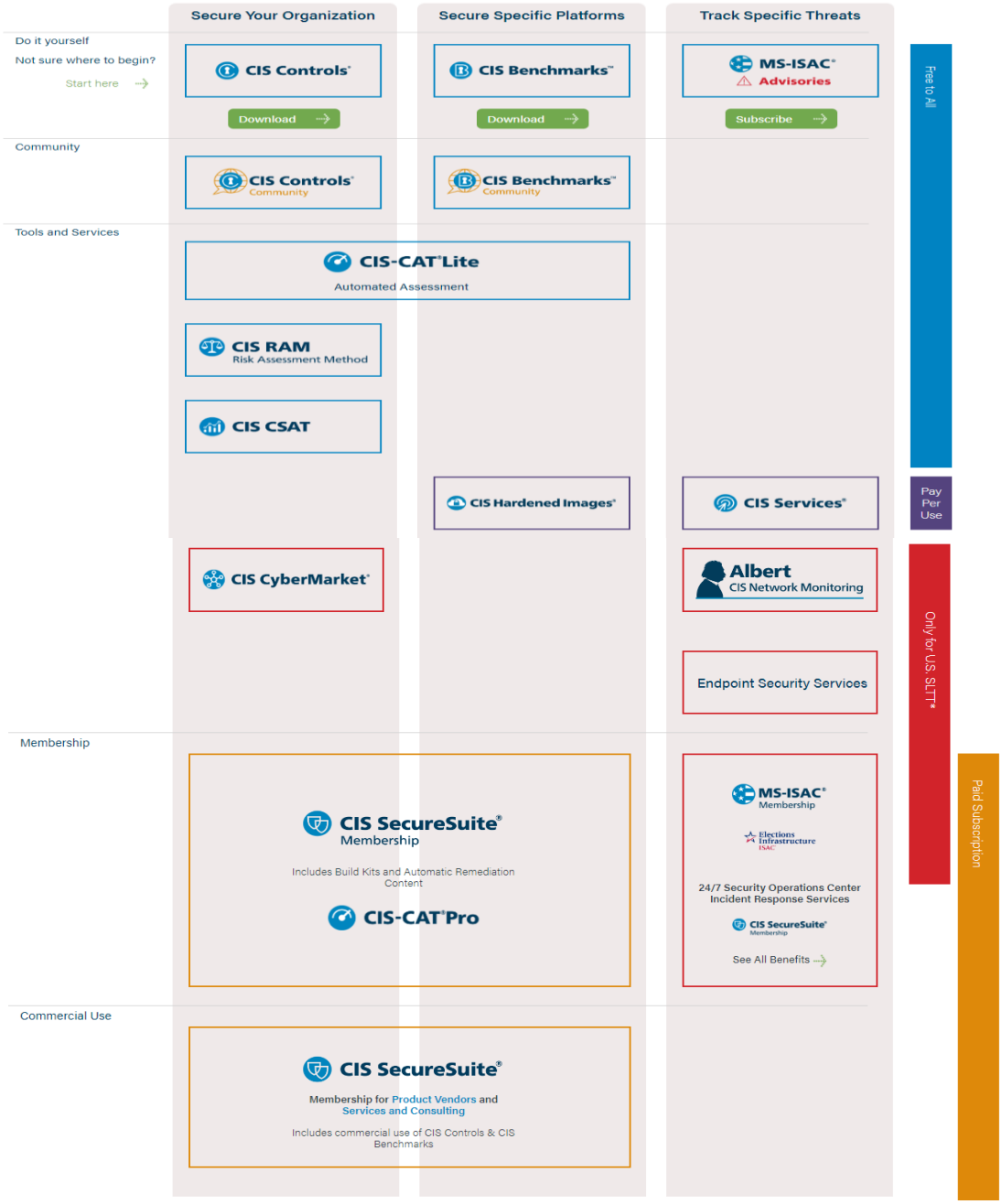


Figura 1: Soluciones desarrolladas por CIS
Fuente: Sitio Web de CIS [9]

Si bien existe una diversa variedad de soluciones que de uno u otro modo apoyan en el proceso de *hardening*, en el presente documento se investigan y desarrollan en profundidad solo aquellas que aportan directamente al tema de estudio.

2.1.1. CIS Benchmarks

Los CIS Benchmarks [10] son guías de configuración de seguridad basadas en el consenso y las “mejores prácticas” desarrolladas y aceptadas por el gobierno, empresas, industria y el mundo académico. Se desarrollan a través de los generosos esfuerzos voluntarios de expertos en la materia, proveedores de tecnología, miembros de la comunidad pública, privada y el equipo de desarrollo de puntos de referencia de CIS.

Los CIS Benchmarks se distribuyen de manera gratuita en formato PDF y existen más de 100 guías, para más de 25 familias de productos de proveedores listados a continuación.

- Desktops & Web Browsers: Apple Desktop OSX, Apple Safari Browser, Google Chrome, Microsoft Internet Explorer, Microsoft Windows Desktop XP/NT, Mozilla Firefox Browser y Opera Browser.
- Dispositivos móviles: Apple Mobile Platform iOS y Google Mobile Platform.
- Dispositivos de red: Agnostic Print Devices, Checkpoint Firewall, Cisco Firewall Devices, Cisco Routers/Switches IOS, Cisco Wireless LAN Controller y Juniper Routers/Switches JunOS.
- Métricas de seguridad: Quick Start Guide y Security Metrics.
- Servidores - Sistemas Operativos: Amazon Linux, CentOS, Debian Linux Server, IBM AIX Server, Microsoft Windows Server, Novell Netware, Oracle Linux, Oracle Solaris Server, Red Hat Linux Server, Slackware Linux Server, SUSE Linux Enterprise Server, Ubuntu LTS Server.
- Servidores - Servicios: Apache HTTP Server, Apache Tomcat Server, BIND DNS Server, FreeRADIUS, Microsoft IIS Server, IBM DB2 Server, Microsoft Exchange, Microsoft SharePoint Server, Microsoft SQL Server, MIT Kerberos, MySQL Database Server, Novell eDirectory,

OpenLDAP Server, Oracle Database Server y Sybase Database Server.

- Plataformas de virtualización y nube: Agnostic VM Server, AWS Foundations, AWS Three-Tier Web Architecture, Docker, Kubernetes, VMware Server y Xen Server.
- Otros: Microsoft Access, Microsoft Excel, Microsoft Office, Microsoft Outlook, Microsoft PowerPoint y Microsoft Word.

La mayoría de los CIS Benchmarks [10] incluyen varios perfiles de configuración. El perfil de nivel 1 se considera una recomendación básica que se puede implementar con bastante prontitud y está diseñado para no tener un gran impacto en el rendimiento; la intención de la evaluación comparativa de este perfil es reducir la superficie de ataque de su organización mientras mantiene las máquinas utilizables y no obstaculiza la funcionalidad comercial. El perfil de nivel 2 se considera "defensa en profundidad" y está destinado a entornos donde la seguridad es primordial; las recomendaciones asociadas con este perfil pueden tener un efecto adverso en su organización si no se implementan adecuadamente o sin el debido cuidado. Finalmente, el perfil STIG (Security Technical Implementation Guides) reemplaza al anterior nivel 3 y proporciona todas las recomendaciones que son específicas de STIG. Cada recomendación dentro de cada CIS Benchmark está asociada con al menos un perfil e independientemente del nivel que se implemente, se recomienda aplicar primero en un entorno de prueba para determinar el impacto potencial.

2.1.2. CIS Build Kits

CIS Build Kits [11] son una serie de objetos de directiva de grupo (GPO) para Windows y scripts para entornos Linux que automatizan el proceso de *hardening*, evitando que el usuario final aplique manualmente las recomendaciones existentes en los CIS Benchmarks. Si bien una demo de los Build Kits de Red Hat Enterpise Linux 7 y Windows 10 pueden ser descargados en [12], para obtener las GPOs y scripts para otros sistemas operativos [13] es necesario una membresía de CIS SecureSuite [14] que tiene un costo para consultores que oscila entre 5.500 a 22.000 $us

americanos y entre 1.452 a 15.598 $us para empresas, costo que debe ser pagado anualmente [15].

2.1.3. CIS CAT

CIS-CAT (CIS Configuration Assessment Tool) [16] es una herramienta de evaluación que ayuda a los usuarios a realizar escaneos y evaluar configuraciones seguras para múltiples tecnologías. Existen dos versiones, la Pro que es de paga y la versión Lite que es gratuita con soporte para los CIS Benchmarks de Windows 10, Ubuntu y Google Chorme; ambas versiones tienen GUI (Interfaz Gráfica de Usuario) y CLI (Interfaz de Línea de Comandos) y genera un reporte en HTML con una puntuación del 1 al 100 asociada al nivel de seguridad del sistema escaneado.

2.2. NIST

El NIST [17] o Instituto Nacional de Estándares y Tecnología (por sus siglas en inglés, National Institute of Standards and Technology) es una agencia del gobierno de los Estados Unidos que opera bajo el Departamento de Comercio y que desempeña un papel fundamental en el avance de la tecnología, la promoción de estándares y la mejora de la seguridad y la calidad en una amplia variedad de sectores industriales. En términos de Seguridad de la información y ciberseguridad, el NIST juega un papel fundamental en el desarrollo de pautas y estándares, como los documentos NIST SP (Special Publication) que son documentos técnicos que abordan una amplia gama de temas como ciberseguridad, criptografía, gestión de riesgos y la seguridad de la información. [18]

2.2.1. National Checklist Program (NCP)

Muchas organizaciones han creado *checklists* (listas de verificación) de seguridad; sin embargo, estas varían ampliamente en términos de calidad, usabilidad, propósito, nivel de seguridad proporcionado y modo de implementación; además, quedan obsoletas a medida que se publican actualizaciones o mejoras de software y puede resultar difícil determinar si un *checklists* está actualizado.

Para facilitar el desarrollo de *checklists* de seguridad para productos de TI y hacer que las listas de verificación estén más organizadas y utilizables, el

NIST estableció el *National Checklist Program* (NCP) [19] que tiene los siguientes objetivos [20]:

- Facilitar el desarrollo y el intercambio de *checklists* proporcionando un marco formal para que los proveedores y otros desarrolladores de listas de verificación las envíen al NIST.
- Proporcionar orientación a los desarrolladores para ayudarlos a crear *checklists* estandarizados y de alta calidad que se ajusten a entornos operativos comunes.
- Ayudar a los desarrolladores y usuarios brindándoles pautas para hacer que los *checklists* estén mejor documentadas y sean más utilizables.
- Alentar a los proveedores de software y otras partes a desarrollar *checklists*.
- Proporcionar un proceso gestionado para la revisión, actualización y mantenimiento de *checklists*.
- Proporcionar un repositorio fácil de usar de información de *checklists*.
- Proporcionar contenido del *checklists* en un formato estandarizado.
- Fomentar el uso de tecnologías de automatización para la aplicación de *checklists*.

La publicación NIST-SP 800-70 [20] está destinado a usuarios y desarrolladores de listas de verificación de configuración de seguridad. Para los usuarios de *checklists*, el documento hace recomendaciones para seleccionar, evaluar, probar y aplicar los *checklist* a productos de TI. Por su parte, para los desarrolladores de listas de verificación, establece las políticas, procedimientos y requisitos generales para la participación en el Programa Nacional de Lista de Verificación (NCP) del NIST.

2.2.2. Security Configuration Checklist

Los *Security Configuration Checklist* [20] (también llamado guía de hardenización o *benchmark*) son una serie de instrucciones o procedimientos para configurar un producto de TI en un entorno operativo particular, verificar que el producto se haya configurado correctamente y/o identificar cambios no autorizados en el producto. El producto de TI puede ser comercial, de código abierto, disponible para el gobierno (GOTS - government-off-the-shelf) u otro.

Normalmente, los *checklist* los crean los proveedores de TI para sus propios productos; sin embargo, otras organizaciones, como el mundo académico, consorcios y agencias gubernamentales, también crean listas de verificación que puede incluir cualquiera de los siguientes:

- Archivos de configuración que establecen o verifican automáticamente varias configuraciones relacionadas con la seguridad (por ejemplo, ejecutables, plantillas de seguridad que modifican la configuración, XML (Lenguaje de marcado extensible) del Protocolo de automatización de contenido de seguridad (SCAP) y scripts).
- Documentación (por ejemplo, archivo de texto) que guía al usuario de la lista de verificación para configurar manualmente un producto de TI.
- Documentos que explican los métodos recomendados para instalar y configurar de forma segura un dispositivo.
- Documentos programáticos y de políticas que establecen pautas para aspectos tales como auditoría, mecanismos de autenticación (por ejemplo, contraseñas) y seguridad perimetral.

El National Checklist Program (NCP) incluye dos grupos principales de listas de verificación:

- Automatizado. Un *checklist* automatizado es aquel que se utiliza a través de una o más herramientas que alteran o verifican automáticamente la configuración en función del contenido de la lista de verificación. Muchas listas de verificación están escritas en lenguaje de marcado extensible (XML) y existen herramientas especiales que pueden usar el contenido de los archivos XML para verificar y alterar la configuración del sistema.
- No Automatizado. Un *checklist no* automatizado es aquel que está diseñado para usarse manualmente, como instrucciones en prosa que describen los pasos que debe seguir un administrador para asegurar un sistema o para verificar su configuración de seguridad.

A continuación se muestran ejemplos de los tipos de dispositivos y software para los que están destinados los c*hecklist* de seguridad:

- Sistemas operativos de propósito general y sistemas operativos móviles.
- Aplicaciones comunes como clientes de correo electrónico, navegadores web, procesadores de texto, firewalls personales y software antivirus.
- Dispositivos de infraestructura como enrutadores, conmutadores, firewalls, puertas de enlace de redes privadas virtuales (VPN), sistemas de detección de intrusiones (IDS), puntos de acceso inalámbrico y sistemas de telecomunicaciones.
- Servidores de aplicaciones como el sistema de nombres de dominio (DNS), el protocolo de configuración dinámica de host (DHCP), web, el protocolo simple de transferencia de correo (SMTP) y servidores de bases de datos.
- Otros dispositivos de red como escáneres, impresoras y fotocopiadoras.

2.2.3. National Checklist Repository

NIST mantiene el *National Checklist Repository* (Repositorio Nacional de Listas de Verificación) [21] , que es un recurso disponible públicamente que contiene información sobre una variedad de *Security Configuration Checklist* para productos o categorías de productos de TI específicos. El repositorio, que se encuentra en https://checklists.nist.gov/, contiene información que describe cada *checklist* y alberga copias de algunas listas de verificación (principalmente las desarrolladas por el gobierno federal de los Estados Unidos de América) o tiene enlaces a la ubicación de otras listas de verificación. Los usuarios pueden navegar y buscar en el repositorio para localizar un c*hecklist* en particular utilizando una variedad de criterios y el repositorio facilita que las organizaciones encuentren las versiones actuales y autorizadas de las listas de verificación de seguridad para determinen cuáles satisfacen mejor sus necesidades.

2.3. SCAP - Security Content Automation Protocol

Un elemento fundamental para el desarrollo del presente trabajo es SCAP - Security Content Automation Protocol, un marco de especificaciones

multipropósito mantenido por el NIST, que admite configuración automatizada, verificación de vulnerabilidades y parches, actividades de cumplimiento de control técnico y medición de seguridad. La familia de estándares SCAP se compone de estándares para múltiples componentes, diseñados para trabajar juntos hacia el objetivo común. Para cada componente, el estándar define un formato de documento con sintaxis y semántica de las estructuras de datos internas. Todos los componentes se basan en el lenguaje de marcado extensible (XML) y cada estándar del componente define su propio espacio de nombres XML [22]. Los siguientes puntos detallan los componentes que conforman el estándar SCAP.

2.3.1. XCCDF - Extensible Configuration Checklist Description Format

El acrónimo XCCDF hace referencia a *Extensible Configuration Checklist Description Format*. Como sugiere el nombre, el lenguaje se utiliza para describir las listas de verificación de seguridad y está diseñado para respaldar el intercambio de información, la generación de documentos, la adaptación organizacional y situacional, las pruebas de cumplimiento automatizadas y la puntuación de cumplimiento. El lenguaje no contiene comandos para realizar el escaneo y es mayoritariamente descriptivo. Se pueden hacer referencia a otros componentes desde el XCCDF (OVAL, OCIL), por lo que se podría llegar a la conclusión de que el XCCDF vincula todos los demás estándares componentes. Si el documento XCCDF se escribe cuidadosamente, es posible lograr un documento que sea portátil entre todas las plataformas de destino y solo los documentos de evaluación (OVAL, OCIL) diferirán. Como todos los lenguajes SCAP, XCCDF se basa en XML y define sus elementos y atributos XML. La especificación del lenguaje describe todos los elementos en detalle y se puede consultar en el NIST IR 7275 Revisión 4.

2.3.2. OVAL - Open Vulnerability and Assessment Language

El acrónimo OVAL significa *Open Vulnerability and Assessment Language*; es un lenguaje declarativo para hacer afirmaciones lógicas sobre el estado del sistema. Es el componente principal del estándar SCAP y se utiliza para describir vulnerabilidades de seguridad o la configuración deseada

de los sistemas. Las definiciones OVAL definen un estado seguro de algunos objetos en una computadora; por ejemplo, archivos de configuración, permisos de archivos, procesos, etc.

OVAL es desarrollado por una comunidad de colaboradores de muchas organizaciones industriales, académicas y gubernamentales. Los documentos OVAL se pueden encontrar en el repositorio OVAL de CIS (Center for Internet Security) [23] y un detalle del estándar está disponible en la Guía [24].

2.3.3. OCIL - Open Checklist Interactive Language

El Open Checklist Interactive Language define un marco para expresar un conjunto de preguntas que se presentarán a un usuario y los procedimientos correspondientes para interpretar las respuestas a estas preguntas. Aunque la especificación OCIL se desarrolló para su uso con listas de verificación de seguridad de TI, los usos de OCIL no se limitan de ninguna manera a la seguridad de TI. Otros posibles casos de uso incluyen encuestas de investigación, exámenes de cursos académicos y tutoriales instructivos.

OCIL se considera una especificación emergente, por lo que actualmente no está incluida en SCAP; sin embargo, se puede utilizar junto con especificaciones SCAP como XCCDF para ayudar a manejar casos en los que los lenguajes de verificación de nivel inferior como OVAL no pueden automatizar una verificación en particular. En resumen, OCIL proporciona un enfoque estandarizado para expresar y evaluar controles de seguridad no automatizados (manuales) [25].

2.3.4. SCE - Script Check Engine

Script Check Engine es una extensión SCAP que permite la ejecución de scripts desde la política SCAP, generando interoperabilidad entre scripts y políticas de seguridad.

Este elemento será fundamental para el desarrollo del presente trabajo dada al permitir referenciar lo scripts que se desarrollen en XCCDF, para lo cual; como se describe en [26], se utilizará el elemento “<check-content-ref>” con “http://open-scap.org/page/SCE” como el atributo “system” y el atributo “href” debe contener la ruta al script.

2.3.5. Source Data Stream

Source Data Stream es un formato que empaqueta otros componentes SCAP en un solo archivo. Esto es útil al distribuir contenido SCAP; por ejemplo, a través de internet, porque un solo archivo es más fácil de manejar. Este formato será fundamental para el desarrollo del sistema propuesto en el presente trabajo.

2.3.6. ARF - Asset Reporting Format

El Formato de Informes de Activos “ARF” por sus siglas en inglés (Asset Reporting Format) consolida varios archivos de resultados (OVAL y XCCDF). A este estándar también se le suele llamar Result DataStream.

2.3.7. CPE - Common Platform Enumeration

El estándar Common Platform Enumeration (CPE) sirve para identificar plataformas y sistemas de TI utilizando nombres definidos de forma inequívoca. CPE también incluye un método para comparar nombres con un sistema y un formato de descripción para vincular texto y pruebas a un nombre. CPE se utiliza en documentos OVAL y XCCDF para identificar la plataforma de destino de verificaciones o definiciones. El diccionario oficial se encuentra en [27] y un ejemplo de CPE de Fedora es “cpe:/o:fedoraproject:fedora:22”.

2.4. SANS Institute

SANS "System Administration, Networking, and Security" Institute [28] [29] es una organización dedicada a la ciberseguridad y la capacitación en seguridad informática fundada en 1989. De manera paralela a la formación y certificación de profesionales, las investigaciones realizadas y publicadas por SANS Institute son muy valiosas; en el presente documento se analizarán diversos *Whitepapers*, *posts* publicados en el blog oficial y especialmente los *checklists* del SANS Score Checklist Project.

2.4.1. SANS Score Checklist Project

El "SANS Score Checklist Project" [29] es una iniciativa de SANS Institute que proporciona listas de control (*checklists*) específicas para evaluar y mejorar la seguridad de sistemas y entornos de TI. Estas listas de control

son diseñadas por expertos en seguridad cibernética del SANS y están destinadas a ayudar a las organizaciones a evaluar y mejorar su postura de seguridad. Cada lista de control se enfoca en un área específica de seguridad y proporciona una serie de pasos, configuraciones recomendadas, prácticas recomendadas y medidas de mitigación de riesgos que una organización puede seguir para fortalecer su seguridad en ese aspecto particular. Algunos ejemplos de listas de control que forman parte del proyecto "SANS Score Checklist Project" son:

- Windows Security Checklist: Una lista de control diseñada para ayudar a endurecer servidores y sistemas que utilizan el sistema operativo Windows.
- Linux Security Checklist: Similar a la lista de control de Windows, pero centrada en sistemas Linux.
- Application Security Checklist: Enfoque en la seguridad de las aplicaciones, incluyendo medidas para proteger aplicaciones web y bases de datos.
- Network Security Checklist: Una lista de control que aborda aspectos específicos de seguridad de red, como configuraciones de firewall, control de acceso y monitoreo de tráfico.
- Cloud Security Checklist: Listas de control específicas para evaluar y mejorar la seguridad en entornos de nube, como AWS, Azure o Google Cloud.

2.5. DISA del Departamento de Defensa de EEUU

El Departamento de Defensa de Estados Unidos “DoD” o “USDOD” por sus siglas en inglés (United States Department of Defense) es un departamento ejecutivo del gobierno federal de Estados Unidos encargado de coordinar y supervisar todas las agencias y funciones del gobierno directamente relacionadas con la seguridad nacional y las Fuerzas Armadas de Estados Unidos. [30]

Por su parte, la Agencia de Sistemas de Información de Defensa "DISA” por sus siglas en inglés (Defense Information Systems Agency); conocida como Agencia de Comunicaciones de Defensa (DCA) hasta 1991, es una

agencia de apoyo al combate del Departamento de Defensa (DoD) de los Estados Unidos compuesta por militares, civiles federales y contratistas. DISA brinda soporte de tecnología de la información (TI) y comunicaciones al Presidente, al Vicepresidente, al Secretario de Defensa, a los servicios militares, a los comandos combatientes y a cualquier individuo o sistema que contribuya a la defensa de los Estados Unidos. [31]

El sitio web DoD Cyber Exchange Public [32]; respaldado y mantenido por DISA, proporciona acceso integral a información, políticas, orientación y capacitación cibernéticas para los profesionales cibernéticos de todo el Departamento de Defensa y el público en general. Entre diversos recursos proporcionados para permitir al usuario cumplir con las reglas, regulaciones, mejores prácticas y leyes federales, publica los Security Requirements Guides (SRGs) y Security Technical Implementation Guides (STIGs) como lineamientos de *hardenización* de diversas tecnologías y proveedores respectivamente de cumplimiento obligatorio de toda organización que forme parte de las redes de información del DoD.

2.5.1. SRGs y STIGs

Las Guías de Requisitos de Seguridad “SRG” por sus siglas en inglés (*Security Requirements Guides*) y las Guías de Implementación Técnica de Seguridad “STIG” (*Security Technical Implementation Guides*) son un compendio de políticas, regulaciones de seguridad y mejores prácticas de configuración desarrollados por DISA, son actualizados trimestralmente y tienen el objetivo de establecer lineamientos de *hardenización* de dispositivos de red, servidores, sistemas operativos, software, aplicaciones, etc. [33]

La diferencia es que los *Security Requirements Guides* “SRG” contienen en su mayoría declaraciones y recomendaciones generales para proteger una tecnología, sin mencionar un tipo o proveedor específico; representando un paso intermedio entre los Identificadores de Correlación de Control (CCI)[3] y las Guías de implementación técnica de seguridad (STIG).

[3] El Identificador de Correlación de Control “CCI” (Control Correlation Identifier) proporciona un identificador estándar y una descripción para cada una de las declaraciones singulares y procesables que componen un control de Aseguramiento de Información (IA) o una mejor práctica de IA definidos en políticas como el SP 800-53 del NIST. CCI permite que un requisito de seguridad que

Por su parte, los *Security Technical Implementation Guides* "STIG" proporcionan información específica de un producto para validar y lograr el cumplimiento de los requisitos definidos en el SRG para el área tecnológica de ese producto, suelen ser específicos del proveedor y detallan reglas (junto con guías de implementación) para sistemas específicos. Por ejemplo, un STIG podría proporcionar configuraciones específicas para Ubuntu 18.04 LTS, mientras que un SRG proporcionaría una guía sobre cómo proteger un sistema operativo en general. [34]

Cada SRG y STIG está compuesto por reglas / requisitos que tienen identificadores (*Group ID, Rule ID, STIG ID*) y un nivel de severidad que corresponde al nivel de riesgo o vulnerabilidad cubierta por dicha regla, la severidad está dada por las siguientes tres categorías [35]:

- CAT I. Los controles / reglas STIG de categoría 1 cubren los entornos con mayor riesgo de explotación grave. Si son explotadas por un ataque malicioso, estas vulnerabilidades son las amenazas más importantes para la red en general. Si no se controlan, es probable que las vulnerabilidades CAT I deriven en afectación a la integridad, confidencialidad o disponibilidad de servicios. Estos se consideran de alta gravedad y deben resolverse primero.
- CAT II. La categoría 2 de STIG cubre las configuraciones o vulnerabilidades que tienen el potencial de resultar en un problema de ciberseguridad. Aunque el riesgo de incidente sigue siendo alto, CAT II no causaría la pérdida inmediata de la integridad del sistema como se describe en CAT I. Estos se consideran de riesgo y gravedad medios y pueden conducir a una vulnerabilidad CAT I si no se controlan.
- CAT III. Los controles / reglas STIG categoría 3 cubren configuraciones que reducen las defensas de un sistema o red si no se controlan. Estos aumentan el riesgo de ataques de ciberseguridad o fallas del sistema, pero no conducirán directamente a ninguno de ellos. Estos se

se expresa en un marco de políticas de alto nivel se descomponga y se asocie explícitamente con las configuraciones de seguridad de bajo nivel que deben evaluarse para determinar el cumplimiento de los objetivos de ese control de seguridad específico. [75]

consideran de bajo riesgo y baja gravedad, aunque pueden conducir a una vulnerabilidad CAT II.

2.5.2. Herramientas de visualización de SRGs y STIGs

Los archivos SRGs y STIGs están categorizados en “Unclassified” y “For Official Use Only”. Los archivos que pertenecen a la categoría “For Official Use Only” están precedidos por “FOUO_” en el nombre, contienen información confidencial y solo pueden ser accedidos por personal del DoD que cuentan con una Tarjeta de Acceso Común “CAC-based PKI certificate” (Common Access Card). Sin embargo, todos los archivos “Unclassified” (que están precedidos por “U_” en el nombre) pueden ser accedidos de manera libre y gratuita desde el sitio DoD Cyber Exchange Public [36]. Estos archivos están en formato XCCDF (Extensible Configuration Checklist Description Format), que es un formato XML que especifica listas de verificación de seguridad, pruebas comparativas y documentación de configuración. El desarrollo de este formato está a cargo del NIST, la NSA, MITRE y el DoD.

Si bien los archivos pueden ser visualizados en un navegador web u otra herramienta que permita visualizar el formato XML, el DoD proporciona la herramienta STIG Viewer (disponible para Windows y Linux) que permite ver uno o más STIG con formato XCCDF en un formato legible por humanos y fácil de navegar; proporcionando una interfaz de usuario gráfica e intuitiva que permite un fácil acceso al contenido de STIG, junto con funciones adicionales de búsqueda y clasificación. [37]

3. HERRAMIENTAS DE HARDENIZACIÓN

Una vez revisadas algunos de los más importantes estándares, guías y lineamientos de hardening, se analiza a continuación herramientas que ayudan al proceso de hardenización.

3.1. OpenSCAP

OpenSCAP (Open Security Content Automation Protocol) es un conjunto de herramientas y estándares de código abierto diseñados para evaluar, medir y garantizar la seguridad de los sistemas. Las principales características y componentes de OpenSCAP son las siguientes [38]:

- Compatibilidad con Estándares Abiertos. Se basa en estándares abiertos, como el estándar SCAP (Security Content Automation Protocol), XCCDF (eXtensible Configuration Checklist Description Format) y OVAL (Open Vulnerability and Assessment Language), para garantizar la interoperabilidad y la adopción generalizada.
- Evaluación de Conformidad. OpenSCAP permite evaluar sistemas y aplicaciones en función a perfiles de cumplimiento de seguridad predefinidos o personalizados. Esto permite verificar si los sistemas cumplen con ciertas políticas de seguridad, como CIS Benchmarks, STIGs, PCI-DSS y más.
- Evaluación de Vulnerabilidades. Permite identificar y evaluar vulnerabilidades de seguridad en sistemas. Utiliza bases de datos de vulnerabilidades comunes y otras fuentes para ayudar en la identificación de riesgos de seguridad.
- Generación de Informes y Resultados Estructurados. Proporciona informes estructurados que ofrecen una visión detallada del estado de seguridad y cumplimiento.
- Escaneo Automatizado y Continuo. Permite la automatización de escaneos de seguridad y evaluaciones periódicas, facilitando la monitorización y el mantenimiento continuo de la postura de seguridad.
- Aplicación de Correcciones y Remedios. Permite la aplicación de correcciones y remedios para abordar las vulnerabilidades y no conformidades detectadas, facilitando la implementación de mejoras de seguridad.

A la comunidad que mantiene el proyecto, le gusta pensar en el ecosistema OpenSCAP en términos de capas, donde los proyectos de nivel superior dependen de los proyectos de nivel inferior. En la capa inferior se encuentra OpenSCAP Base, que proporciona la funcionalidad básica de leer contenido SCAP, permite realizar escaneos de cumplimiento en un solo sistema y cuenta con el escáner de línea de comandos certificado por NIST llamado “oscap”. Una capa arriba se encuentra SCAP Workbench, una interfaz gráfica de usuario que utiliza la funcionalidad proporcionada por OpenSCAP Base, su objetivo es ser intuitivo y reducir la curva de aprendizaje

inicial del escaneo SCAP. OpenSCAP y SCAP Workbench son útiles para escanear y posiblemente reparar sistemas ya instalados y en ejecución, pero ¿qué sucede si se desea instalar uno nuevo y garantizar su cumplimiento desde el principio? aquí es donde entra en juego el complemento OpenSCAP Anaconda, que se integra en el instalador de Anaconda y permite instalar un nuevo sistema que cumplirá con su política desde el primer inicio. Aún más arriba en la jerarquía se encuentra el demonio OpenSCAP, que permite escanear continuamente múltiples sistemas, ya sea que se ejecuten sin sistema operativo o como máquinas virtuales, e incluso puede realizar escaneos de cumplimiento de contenedores. En el nivel más alto del ecosistema hay varias herramientas que permiten mantener múltiples sistemas en un estado de cumplimiento de seguridad como Spacewalk, Foreman o Cockpit; las herramientas de nivel inferior proporcionadas por el proyecto OpenSCAP pueden funcionar de manera confiable con cualquiera de estos marcos de administración de sistemas. [39]

Finalmente, es importante aclarar que el enfoque de OpenSCAP en SCAP, no significa que sea el único estándar que toma en cuenta; así pues, la comunidad que lidera el proyecto descubre proactivamente nuevos estándares y evalúa posibilidades para extender OpenSCAP para que sea interoperable con ellos. Algunos de los estándares adicionales que considera son FISP (del NIST), Common Criteria (certificación de software de seguridad informática), SWID (etiquetas de identificación de software) y SACM (propuesto a través de un grupo de trabajo del IETF). [40]

3.1.1. OpenSCAP Base

Como se vio en el punto previo, la herramienta de la capa más baja es OpenSCAP Base, que proporciona “oscap”, una herramienta de línea de comandos que tiene el objetivo principal de realizar análisis de configuración y vulnerabilidad de un sistema local; ayudando en gran medida en la evaluación de DISA STIG, USGCB de NIST o Red Hat Security Response Team y que puede evaluar flujos de datos de origen SCAP, puntos de referencia XCCDF o definiciones OVAL. [41]

El manual de usuario de OpenSCAP [42] [43] describe en detalle todas las funcionalidades de “oscap”, entre las que destacan la posibilidad de remediar automáticamente los sistemas que se han encontrado en un estado que no cumple con las normas. Para la corrección del sistema, las reglas del contenido SCAP deben tener adjunto un script de corrección, como ocurre con los *SCAP source data streams* del paquete *scap-security-guide*. La reparación del sistema consta de los siguientes pasos:

- El comando “oscap” realiza una evaluación XCCDF.
- Se realiza una evaluación de los resultados evaluando las definiciones OVAL y cada regla que ha fallado se marca como candidata a corrección.
- “oscap” busca un elemento <xccdf:fix> apropiado , lo resuelve, prepara el entorno y ejecuta el script de reparación.
- Cualquier resultado del script de corrección es capturado por “oscap” y almacenado dentro del elemento <xccdf:rule-result>. Además, el valor de retorno del script de reparación también se almacena.
- Siempre que “oscap” ejecuta un script de corrección, inmediatamente evalúa nuevamente la definición de OVAL (para verificar que el script de corrección se haya aplicado correctamente). Durante esta segunda ejecución, si la evaluación OVAL arroja éxito, el resultado de la regla es *fixed*, de lo contrario es *error*.
- Los resultados detallados de la corrección se almacenan en un archivo XCCDF de salida y contiene dos elementos <xccdf:TestResult> . El primer elemento <xccdf:TestResult> representa el análisis previo a la corrección, el segundo <xccdf:TestResult> se deriva del primero y contiene resultados de corrección.

Hay tres modos de funcionamiento de oscap con respecto a la remediación:

- En línea. Los scripts de corrección se ejecutan al momento del escaneo, para este modo de funcionamiento se utiliza la opción “--remediate” en la ejecución del comando.

- Fuera de línea. En este modo de funcionamiento primero se ejecuta el comando de evaluación y posteriormente un segundo comando de remediación.
- Revisión. Este modo consiste en realizar la evaluación y exportar las instrucciones de remediación en un archivo bash que posteriormente será ejecutado como un script.

Otra alternativa de difusión de correcciones sin realizar una evaluación previa es la generación de script bash o Playbooks de Ansible desde un perfil XCCDF. Los comandos a ejecutar para cada caso son “oscap xccdf generate fix --profile ospp /usr/share/xml/scap/ssg/content/archivo-deseado.xml > fix.sh” u “oscap xccdf generate fix --profile ospp --fix-type ansible /usr/share/xml/scap/ssg/content/archivo-deseado.xml > playbook.yml” respectivamente.

3.1.2. SCAP Security Guide

SCAP Security Guide es un proyecto de código abierto que consiste en políticas de seguridad escritas en forma de documentos SCAP, para implementar pautas de seguridad recomendadas por entidades reconocidas, entre las que se encuentran STIG, USGCB y PCI DSS. La guía consta de reglas con una descripción muy detallada e incluye scripts de remediación probados y optimizados para los sistemas de destino. [44]

La instalación en Ubuntu se la realiza con la ejecución del comando “apt install ssg-base ssg-debderived ssg-debian ssg-nondebian ssg-applications” y una vez instalada todas las políticas de seguridad de SCAP Security Guide están en el directorio “/usr/share/xml/scap/ssg/content/”. Adicionalmente, el listado y enlace a las políticas está disponible en [45].

3.1.3. Openscap-utils y oscap-ssh

El paquete “openscap-utils” contiene herramientas de línea de comandos creadas sobre la biblioteca OpenSCAP [46]. En el presente trabajo será de gran utilidad la herramienta “oscap-ssh” del paquete “openscap-utils”, ya que permite escanear máquinas remotas a través de la red.

En detalle, “oscap-ssh” ejecuta la herramienta “oscap” en un sistema remoto a través de una conexión SSH, los archivos de entrada se transfieren al sistema de destino y una vez finalizado el análisis, los archivos de resultados se transfieren nuevamente, por lo que no quedan datos temporales en la máquina remota. La herramienta requiere bash, ssh, scp y mktemp para realizar evaluaciones OVAL y XCCDF de máquinas remotas, además que la máquina remota también debe tener instalado “oscap” y en estar referenciada en el $PATH, lo cual se puede lograr instalando “openscap” u “openscap-scanner”. [47]

3.1.4. SCAP Workbench

SCAP Workbench es una herramienta con interfaz gráfica que permite abrir archivos XCCDF, Source Data Stream, SCAP RPM o sus variantes bzip2 y ayuda al usuario a evaluar el cumplimiento de un perfil en una máquina local o remota. Entre sus principales características destacan las siguientes: [48]

- Compatibilidad con XCCDF 1.1 y 1.2
- Soporte de Source DataStream 1.2
- Soporte de archivos XCCDF 1.2 Tailoring
- Evaluación de la máquina local
- Evaluación de máquina remota (usando SSH)
- Soporte de personalización limitado: selección, deselección y valor establecido
- Guardar resultados como XCCDF 1.1 o 1.2 (dependiendo de la entrada) o ARF 1.1
- Cargando paquete de contenido desde RPM
- Exportar paquete de contenido como RPM o en una carpeta

Adicionalmente, la herramienta permite corregir las reglas que no se cumplieron en el análisis o exportar una función de reparación a uno de los siguientes archivos: script Bash, manual de Ansible o manifiesto de Puppet, el cual contendrá todas las correcciones para las reglas seleccionadas por el perfil que estén disponibles. [48]

Si bien esta herramienta parece realizar las mismas tareas que el sistema propuesto en el presente trabajo, en el desarrollo y uso del sistema

se evidenciará que SCAP Workbench no presenta la misma facilidad de uso y no permite implementar un proceso evolutivo de hardening de manera nativa y trasparente.

3.2. Ubuntu Security Guide (USG)

La Guía de Seguridad de Ubuntu “USG” por sus siglas en inglés (Ubuntu Security Guide) es una herramienta disponible con Ubuntu 20.04 LTS que facilita en gran medida la hardenización y la auditoría de guías de implementación técnica de seguridad como lo son CIS Benchmark y DISA-STIG. [49]

La herramienta USG forma parte de Ubuntu Advantage y Ubuntu Pro y se instala mediante la herramienta Ubuntu Advantage [50]. En términos de auditoria, permite una revisión a través del comando “$ sudo usg audit <PROFILE> / disa_stig” y con el comando “$ sudo usg fix <PROFILE> / disa_stig” se aplican todas las configuraciones que permiten el cumplimiento de uno de los perfiles que plantea DISA STIG o CIS (cis_level1_workstation, cis_level1_server, cis_level2_ workstation o cis_level2_server). Además, con el objetivo de contar con un script y evitar instalar la herramienta USG en todos los dispositivos y servidores, se puede utilizar el comando “$ sudo usg generate-fix <PROFILE> --output fix.sh”, los detalles técnicos y parametrizaciones de la herramienta está disponible en la documentación publicada por Ubuntu [51] [52] [53] [54] [55].

3.3. Bastille Linux

El proyecto Bastille Linux tiene como objetivo proporcionar una herramienta interactiva de hardenización basada en las mejores prácticas de seguridad ampliamente aceptadas como lo son las guías de SANS Securing Linux, la guía de seguridad del administrador de Linux de Kurt Seifried y otras fuentes de seguridad acreditadas. Si bien la herramienta presenta una interfaz interactiva, los cambios que Bastille Linux puede realizar en un sistema Ubuntu pueden potencialmente dejar inoperativas partes de su sistema o tener otros efectos adversos, por lo que no está recomendada para principiantes, sino más bien para usuarios intermedios y avanzados. En [56] está disponible una guía de instalación y uso, pero en términos generales, el

paquete incluye una interfaz de usuario y un motor de configuración; la interfaz de usuario principal es una interfaz X que utiliza el sistema Perl/Tk y hay una interfaz de texto. Bastille Linux puede ser utilizado en dos modos principales:

- Interactivamente. Bastille Linux realiza una serie de preguntas, con explicaciones del concepto involucrado y fortalece el sistema de acuerdo con sus respuestas a esas preguntas.
- De forma no interactiva. También permite editar un archivo de configuración que luego se usa con Bastille Linux para aplicar las medidas de refuerzo de seguridad. Esta es una manera práctica de automatizar el refuerzo de varios servidores.

3.4. Lynis

Lynis es una herramienta de código abierto con licencia GPL, empleado para realizar auditorías de seguridad, pruebas de cumplimiento (como PCI, HIPAA o SOX), pruebas de penetración, detección de vulnerabilidades y hardenización de sistemas operativos Linux, macOS u otros sistemas basados en Unix. [57]

Esta herramienta desarrollada y mantenida por CISO FY es modular y "oportunista", lo que quiere decir que sólo utiliza y prueba los componentes que encuentra en el sistema y sus bibliotecas; por lo que no es necesaria la instalación de otras herramientas, manteniendo el sistema limpio. Lynis realiza cientos de pruebas individuales, la mayoría de las cuales están escritas en un script de shell y tienen un identificador único (por ejemplo, KRNL-6000); estos scripts se encuentran en [58]. El código está disponible en GtiHub [59] y un manual de usuario es publicado por CISO FY [60].

3.5. Herramientas disponibles en GitHub

GitHub es un portal web que implementa el sistema de control de versiones Git y su objetivo principal es servir de repositorio código de aplicaciones y herramientas de cualquier persona que tenga una cuenta, una de las ventajas es que los proyectos públicos son libres de descarga y en general tienen buena documentación que permiten entender su funcionamiento e inclusive colaborar en el desarrollo. Entre los diferentes proyectos disponibles en GitHub, hay algunas herramientas de *hardening* que

serán muy útiles en el desarrollo del presente trabajo; se mencionan algunas de ellas a continuación.

3.5.1. Repositorio JShielder de Jsitech

JSHielder es un script Bash de código abierto desarrollado para ayudar a SysAdmin y desarrolladores a proteger los servidores Linux en los que implementarán una aplicación o servicio web. Esta herramienta automatiza el proceso de instalación de todos los paquetes necesarios para alojar una aplicación web y hardenizar un servidor Linux con poca interacción por parte del usuario. [61]

En [62] se encuentra un manual detallado de cada comando ejecutado en el script y un elemento muy importante para el presente trabajo es que Jason Soto (el desarrollador) agregó en el repositorio de GitHub [61] otro script Bash para realizar las configuraciones de hardenización descritas en la guía de CIS Benchmark para Ubuntu.

3.5.2. Repositorio Hardening Ubuntu de Konstruktoid

Thomas Sjögren, que tiene asociado el usuario “konstruktoid” publicó en [63] el repositorio “Hardening Ubuntu. Systemd Edition”, que contiene una serie de scripts Bash para evaluar con Lynis y OpenSCAP el cumplimiento de Ubuntu CIS Benchmark, así como hardenizar el servidor ejecutando el script “ubuntu.sh” tomando las configuraciones del archivo “ubuntu.cfg”.

3.5.3. Repositorio GrapheneX

El proyecto “GrapheneX - Automated System Hardening Framework for Linux & Windows”, disponible en [64] y desarrollado en Python, tiene como objetivo proporcionar un Framework para proteger un sistema y/o un servidor web con comandos de hardening automatizados. El software puede ser descargado con el comando “*pip install graphenex*” y ser utilizado a través de la línea de comandos o haciendo uso de su interfaz web, permitiendo hardenizar distintos elementos a través de módulos agrupados en los siguientes *namespaces: “Firewall”, “User”, “Network”, “Services”, “Kernel”, “Filesystem” u “Other”.*

3.6. Soluciones de paga

Como se evidenció en el desarrollo del presente documento, existen diversas guías y herramientas que ayudan en el proceso de hardenización; si bien son gratuitas o de código abierto, son esfuerzos aislados que se deben analizar y seleccionar para utilizar uno o algunos de ellos. Sin duda este problema fue identificado por grandes corporaciones que plantearon soluciones de paga, se analiza a continuación algunas de ellas.

3.6.1. CalCom Hardening Solution (CHS) de CalCom

CalCom [65] es una empresa comercial privada con sede en Israel fundada en 2001. Su principal producto, CalCom Hardening Suite (CHS) [66] es una solución de *hardening* de servidores automatizada diseñada para reducir los costos operativos y aumentar la seguridad y el cumplimiento del servidor. CHS elimina las interrupciones y reduce los costos de hardenización al indicar el impacto de un cambio de configuración de seguridad en los servicios de producción. Garantiza un entorno de servidor resistente, constantemente reforzado y monitoreado.

La solución ofertada es de paga, con un costo anual de 240 dólares americanos por servidor, siendo el paquete mínimo de compra 100 licencias, más un costo de consultoría de implementación de 100 horas por 16.500 dólares; haciendo un total de 40.500 dólares por implementación y 24.000 dólares anuales por renovación de licenciamiento. [67]

La solución trabaja con la instalación de agentes en los servidores a hardenizar, servidores de administración y *gateways* que son implementados siguiendo la siguiente arquitectura de referencia:

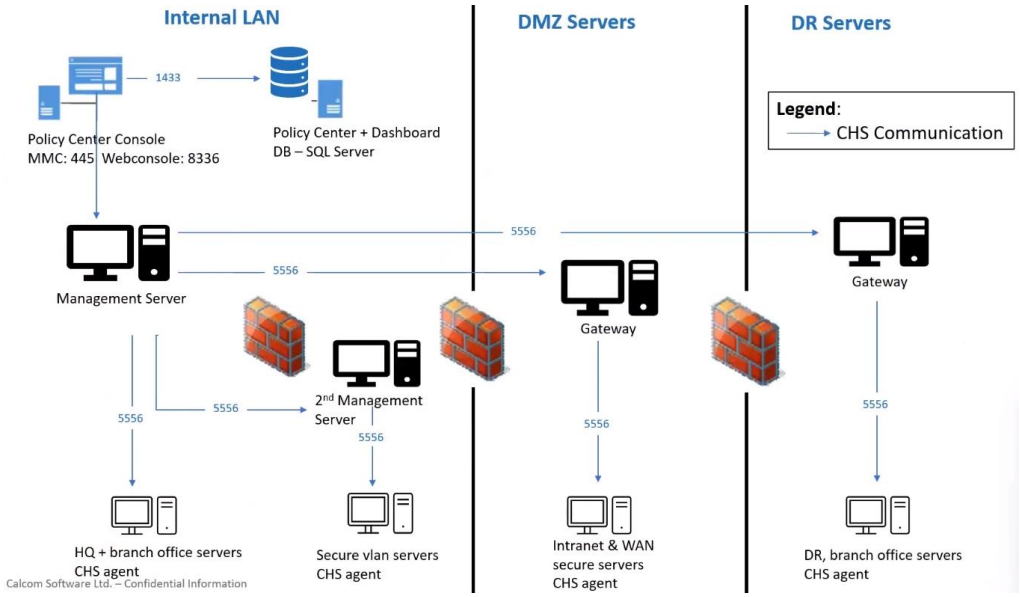


Figura 2: Arquitectura referencial de CalCom CHS
Fuente: Reunión [67]

Una ventaja de CalCom CHS es que sigue el siguiente proceso:

Figura 3: Proceso de Hardening con CalCom CHS
Fuente: Reunión [67]

En una primera etapa el administrador establece las políticas a aplicar; posteriormente, por un periodo inicial de 3 a 4 semanas pasa una etapa en "Modo aprendizaje", en la cual entiende el comportamiento del servidor y los servicios publicados y permite al usuario seleccionar las políticas a aplicar en base a resultados como los que se muestran a continuación:

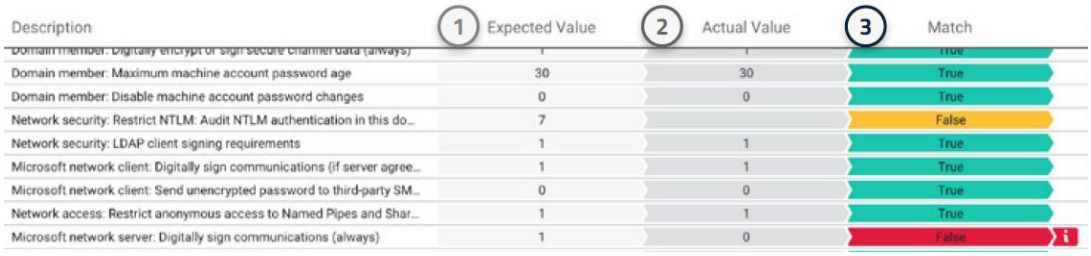


Figura 4: Proceso de Hardening con CalCom CHS
Fuente: Reunión [67]

Donde cada política podrá estar en uno de los siguientes estados de coincidencia (Match):

- Verdadero. Los valores esperados y reales son idénticos.
- Falso (en color amarillo): El valor se modificará al aplicar la política, sin que afecte al funcionamiento del servidor.
- Falso (en color rojo): El sistema de producción utiliza el objeto y su valor real es válido, por lo tanto, el hardening de la política causará daños a los servidores en producción.

En esta etapa denominada “Modo de Aplicación”, el administrador selecciona aquellas políticas que desea configurar en el servidor, pudiendo establecer una justificación para aquellas políticas no aplicadas. Finalmente en el “Modo supervisión”, tras haber realizado el despliegue de las políticas, permite un monitoreo continuo a través de un *dashboard* de cumplimiento en “CalCom Policy Analysis Center”.

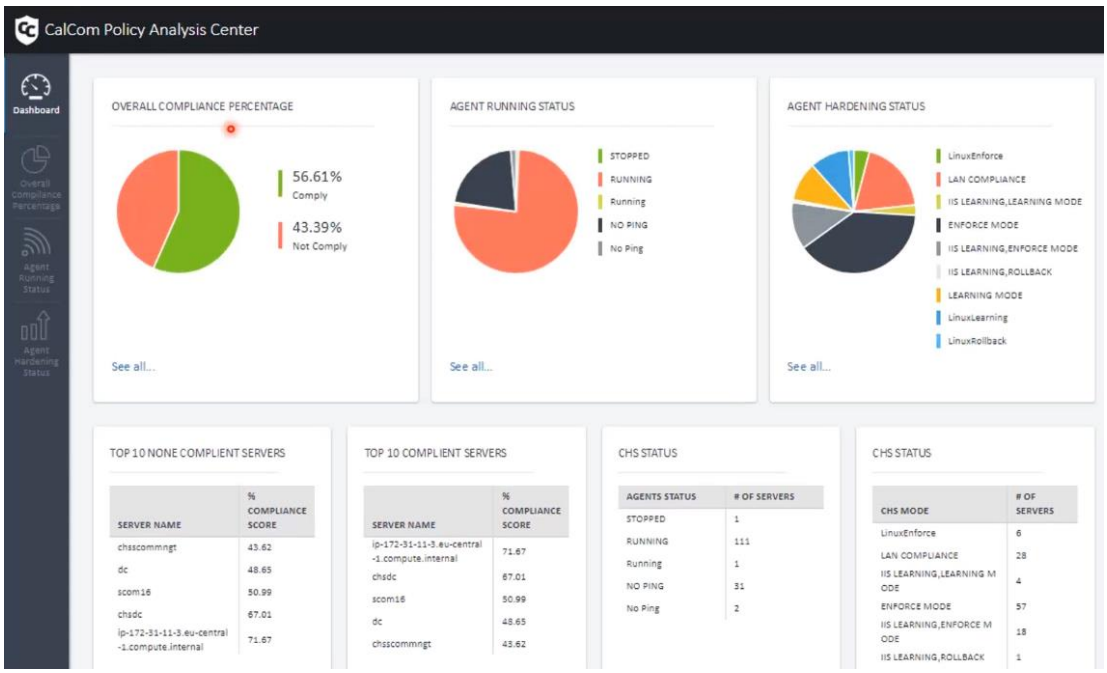


Figura 5 CalCom Policy Analysis Center
Fuente: Reunión [67]

3.6.2. Runecast Analyzer de Runecast

Runecast es una empresa fundada en 2014, con sede en Londres, Reino Unido y un centro de desarrollo en República Checa [68]. Su solución “Runecast Analyzer” es una herramienta de análisis y gestión de riesgos de

Tecnología de Información que se utiliza para evaluar y garantizar la seguridad y conformidad en entornos de infraestructura virtualizada. Está diseñada para trabajar con entornos basados en tecnologías como VMware, Amazon AWS, Microsoft Azure y Kubernetes. Las principales funciones y capacidades de Runecast Analyzer incluyen [69]:

- Cumplimiento de Normativas y Estándares de Seguridad. Ayuda a garantizar el cumplimiento de diversas normativas de seguridad y estándares, como CIS Benchmarks, DISA STIGs, GDPR, HIPAA y otros. Además, proporciona recomendaciones específicas para cumplir con estos estándares.
- Análisis Automatizado de Seguridad y Cumplimiento. Realiza análisis automáticos de seguridad, cumplimiento y riesgos en entornos de TI. Compara la configuración actual con las mejores prácticas de seguridad y conformidad específicas para tecnologías como VMware, AWS, Azuer y Kubernetes.
- Identificación de Vulnerabilidades y Riesgos de Seguridad. Detecta y presenta vulnerabilidades conocidas, configuraciones inseguras y riesgos potenciales en la infraestructura virtualizada. Proporciona información detallada sobre cómo abordar y remediar estos problemas.
- Generación de Informes y Auditorías. Genera informes detallados que resumen el estado de seguridad y cumplimiento, destacando áreas de mejora y proporcionando información para auditorías de seguridad y revisiones periódicas.

De todas las funcionalidades ofrecidas por Runecast, para el presente trabajo se prestará especial atención a los módulos que permiten evaluar el cumplimiento de estándares / guías de seguridad y automatizar el proceso de hardenización. Para ello se accedió al demo en línea disponible en https://demo.runecast.com/rca/issues/detected y se revisó la documentación en línea [70], donde se pudo identificar que la solución puede trabajar en una solución con agentes (implementando osquery) o sin agentes.

El primer elemento para analizar es la opción “Dashboard” del menú lateral, donde se puede identificar el nivel de cumplimiento de normativas / estándares, como se muestra a continuación:

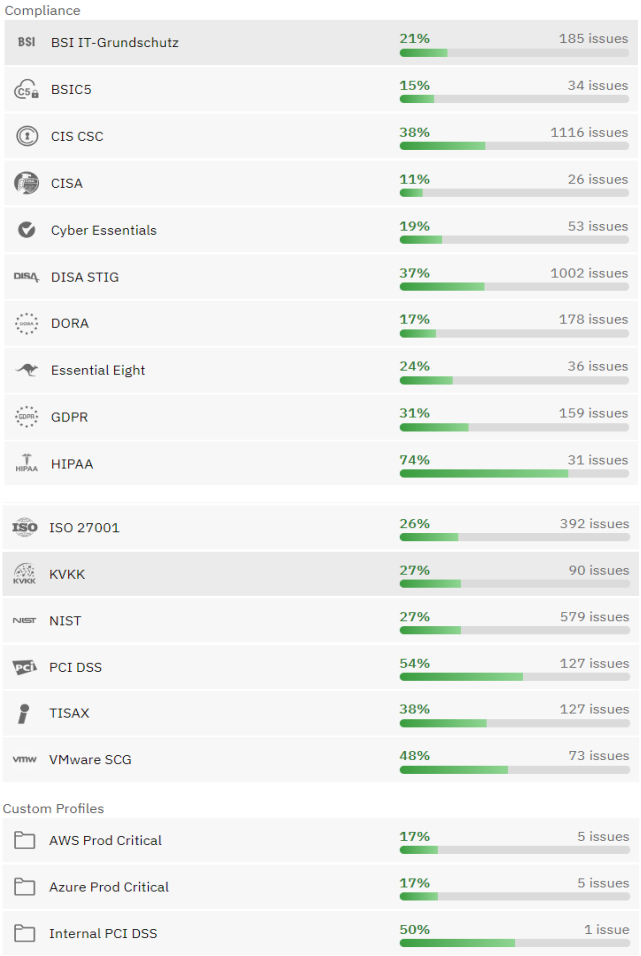


Figura 6: Dashboard Runecast
Fuente: Demo Runecast *[71]*

Un segundo elemento para tomar en cuenta es el inventario de servidores, donde además se puede visualizar las reglas aplicadas y su nivel de cumplimiento.

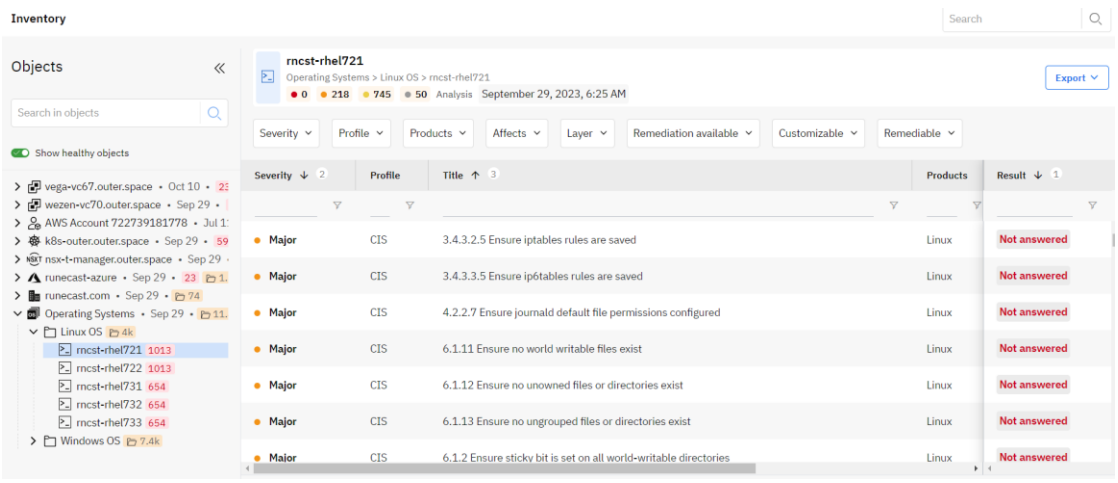


Figura 7: Inventario Runecast
Fuente: Demo Runecast *[71]*

Otro módulo interesante para tomar en cuenta de la herramienta es la gestión de perfiles, donde se pueden configurar y parametrizar perfiles que están conformados por reglas.

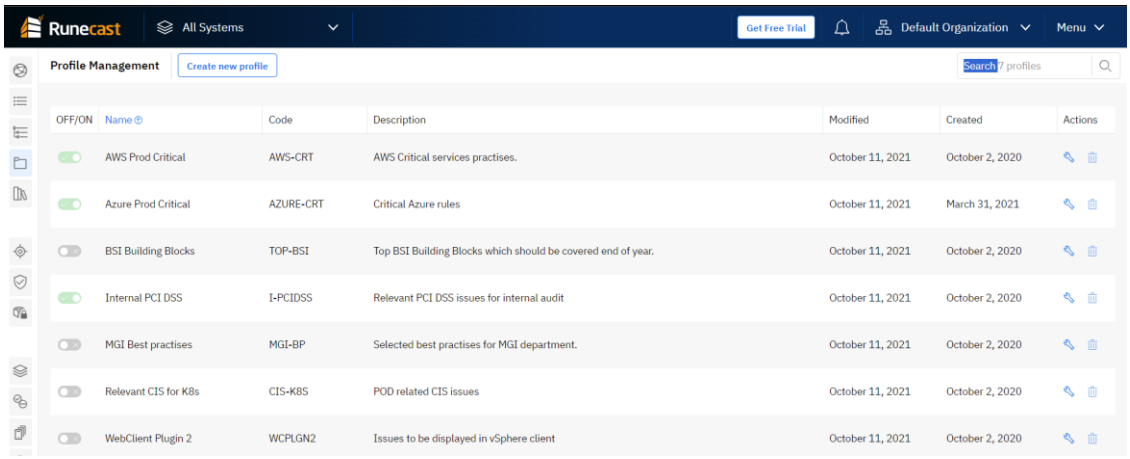
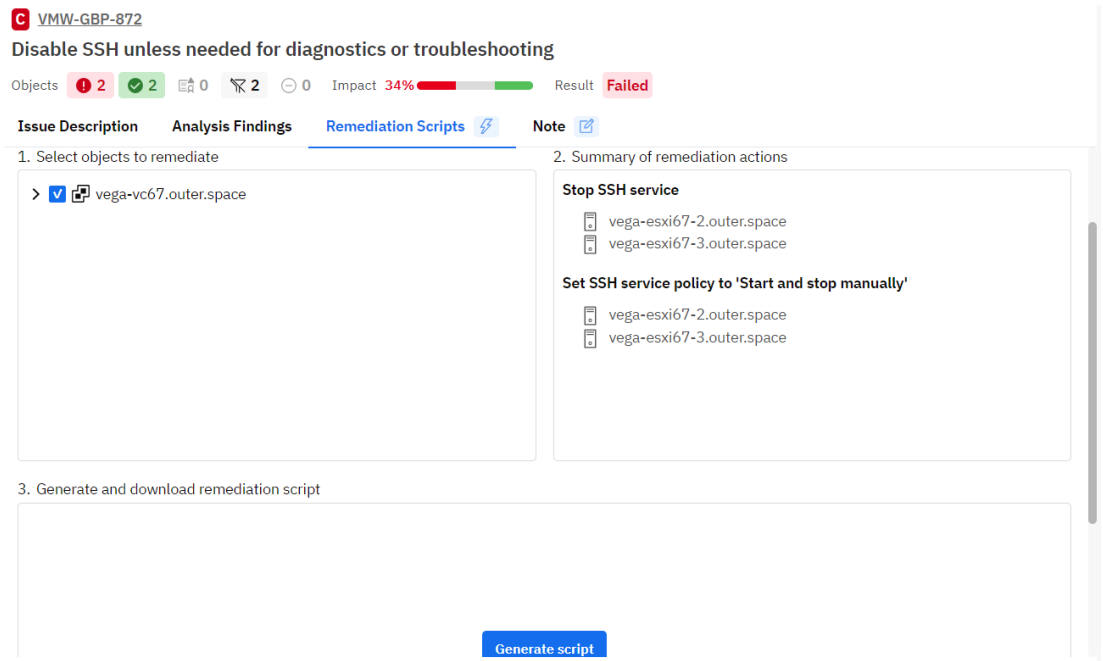


Figura 8: Gestión de perfiles Runecast
Fuente: Demo Runecast *[71]*

Finalmente, un cuarto elemento a considerar es el módulo que permite la remediación de hallazgos; si bien este módulo no está directamente relacionado con elementos de configuración que permitan hardenizar servidores para incrementar el cumplimiento de normativas o estándares, sino a configuraciones asociadas a mejores prácticas para diferentes productos, es importante notar que algunas reglas de la herramienta permiten generar scripts para remediar el hallazgo.



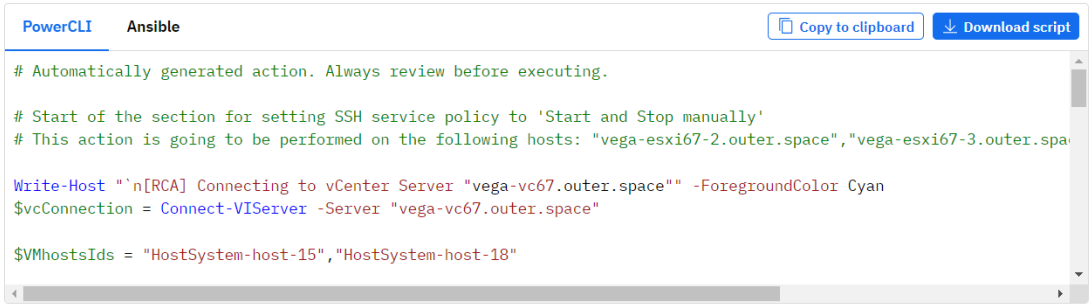


Figura 9: Remediación Runecast
Fuente: Demo Runecast *[71]*

3.6.3. ConfigOS Command Center de SteelCloud

ConfigOS es desarrollado por SteelCloud. Se trata de una aplicación de escritorio desarrollada para Windows, de alto rendimiento y fácil de usar que automatiza el *hardening* de infraestructura tomando como base los estándares DISA STIG o CIS Benchmark.

La Guía de usuario [72] detalla cada uno de los módulos de la herramienta y plantea el siguiente flujo: “Los nuevos usuarios deben progresar a través del flujo de trabajo de forma lineal, comenzando por agregar nuevos endpoints en el panel configuración de endpoints y avanzando a través de “Scan and Remediate” hasta el panel “Resultados” donde se pueden revisar informes y crear listas de verificación. Finalmente, puede avanzar al panel “Revertir” para revertir uno o más trabajos de remediación para corregir los controles de políticas (STIG, CIS, etc.) que pudieran entrar en conflicto con una o varias aplicaciones instaladas en el endpoint. Este proceso puede repetirse varias veces con el fin de contar con endpoints hardenizados”.

El módulo de configuración de endpoints y grupos permite añadir dispositivos Windows, Linux y CiscoIOSXE. La solución es *agent-less*, por lo que la conexión, escaneo y configuraciones las realiza a través de conexiones remotas a los dispositivos, utilizando cuentas con privilegios de administración. Un aspecto interesante a analizar para el presente trabajo es que los dispositivos pueden ser agrupados en grupos y existen íconos que muestran el estado y versión del dispositivo como se plasma a continuación.

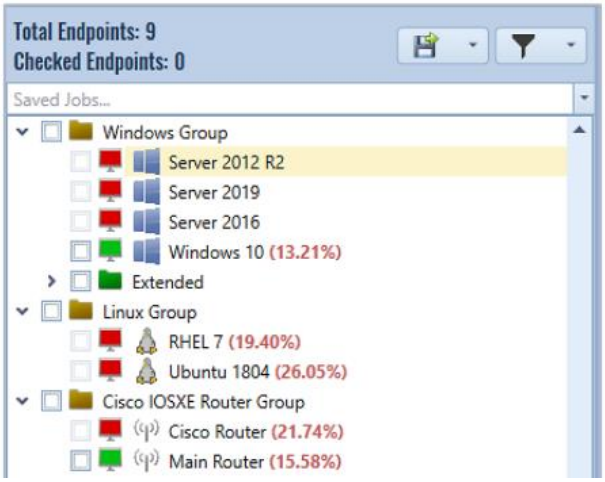


Figura 10: Grupos y endpoints de ConfigOS
Fuente: Guía de Usuario ConfigOS *[72]*

Una vez agregado el *Endpoint* y seleccionada la política que aplicará, se puede escanear, remediar o ejecutar ambas acciones como se muestra a continuación.

Figura 11: Escaneo y Remediación con ConfigOS
Fuente: Guía de Usuario ConfigOS [72]

Una característica muy interesante de esta herramienta es su módulo de “Rollback”, que permite volver a un estado previo a la ejecución de configuraciones de hardenización; lo cual es fundamental tomando en cuenta que algunas configuraciones podrían afectar el normal funcionamiento de algún servidor o servicio publicado por éste y será necesario revertir lo aplicado.

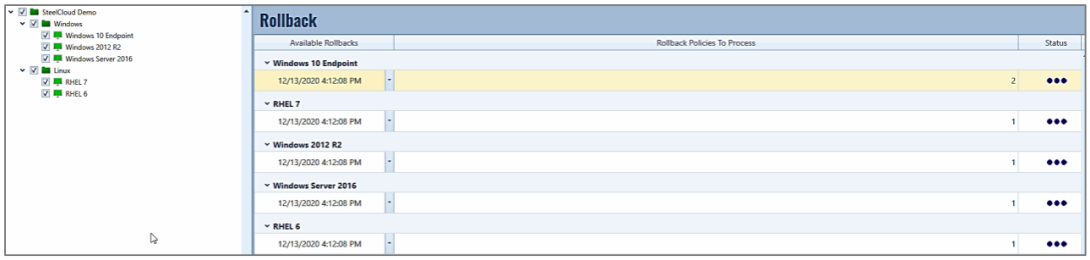


Figura 12: Rollback con ConfigOS
Fuente: Guía de Usuario ConfigOS [72]

Un elemento interesante en el módulo de “Resultados y reportes” es la factibilidad de revisar los resultados históricos, lo cual sería útil para medir el grado de madurez y revisar el historial de hardenización a lo largo del tiempo.

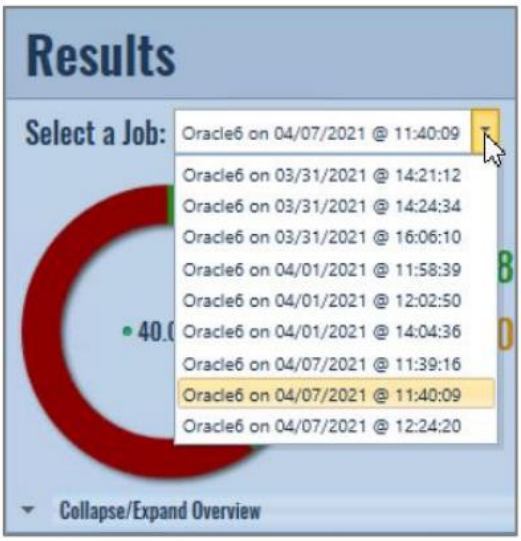


Figura 13: Rollback con ConfigOS
Fuente: Guía de Usuario ConfigOS [72]

Finalmente, el módulo “ConfigOS Job Automation System (JAS)” permite la automatización de tareas repetitivas, programado la ejecución de escaneos y/o remediaciones en periodos y horarios de manera periódica.

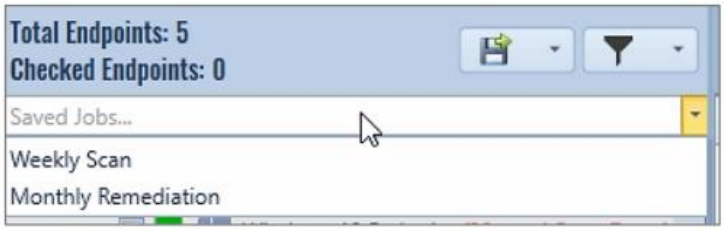


Figura 14: Job Automation System de ConfigOS
Fuente: Guía de Usuario ConfigOS [72]

4. SISTEMA DE HARDENING PROPUESTO

Tras haber revisado conceptos, estándares, guías, herramientas libres y soluciones de paga, se procede a diseñar y desarrollar un sistema que permita a los administradores de infraestructura y sistemas, llevar a cabo un proceso de hardening centralizado, sin agentes y sencillo, basado en estándares y configuraciones de seguridad en formato “Souce Data Stream” (SCAP) elaboradas y actualizadas constantemente por comunidades, organizaciones privadas y entidades gubernamentales reconocidas.

4.1. Diseño del Sistema

El sistema debe ser fácil de utilizar e intuitivo; los módulos con los que podrá interactuar el usuario final son los siguientes:

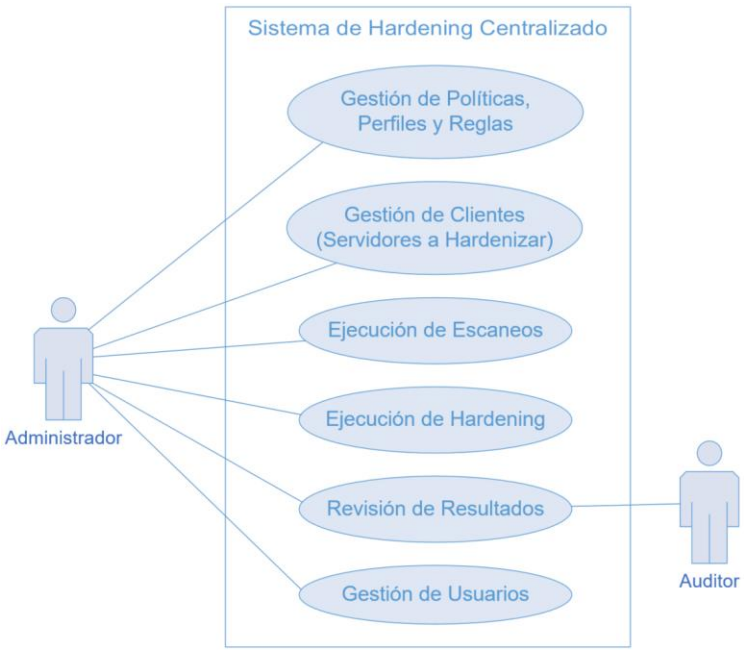


Figura 15: Diagrama de caso de uso del sistema de hardening centralizado
Fuente: Elaboración propia

Desde un nivel de abstracción muy alto, los pasos a seguir en el sistema para llevar a cabo el proceso de hardening son los siguientes:

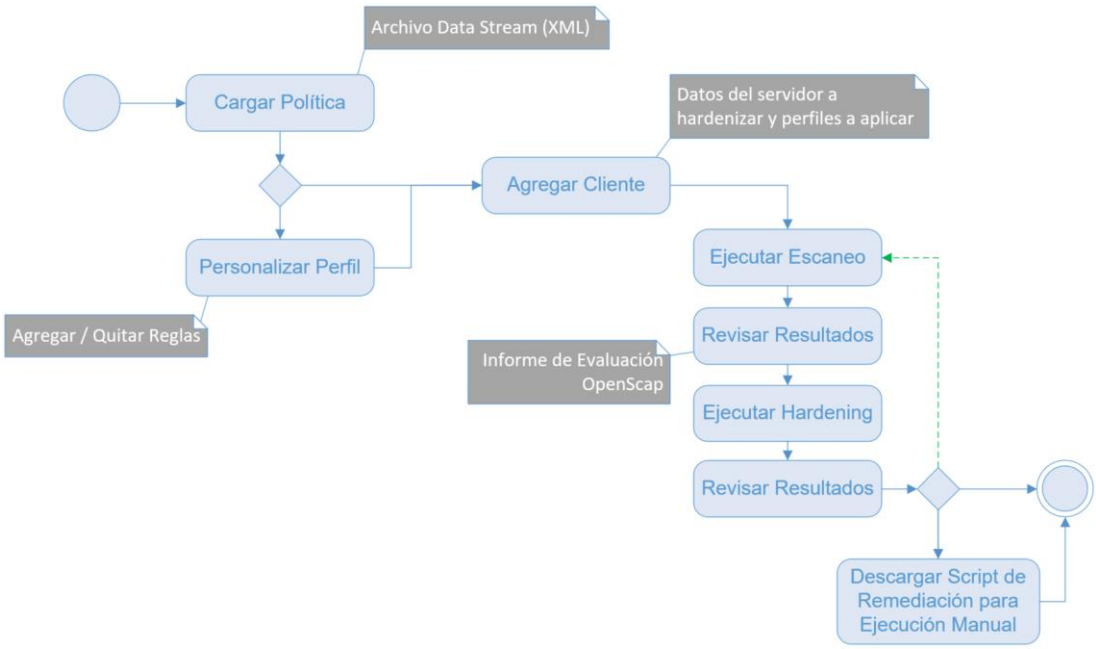


Figura 16: Diagrama de actividades de uso del sistema
Fuente: Elaboración propia

Como se evidencia en el diagrama, existe una línea punteada verde que representa el proceso continuo de hardening de servidores; tarea que se hace bastante sencilla con el sistema ya que el administrador tras haber agregado el cliente a hardenizar y haberle asociado un perfil, tan solo deberá pulsar dos botones (“Ejecutar Escaneo” y “Ejecutar Remediación”) para ir mejorando la seguridad del cliente de manera evolutiva.

Una vez entendido el funcionamiento general del sistema, se detalla a continuación el funcionamiento de los principales módulos.

4.1.1. Gestión de Políticas, Perfiles y Reglas

Tal como lo establece la especificación SCAP, una política está conformada por perfiles y éstos están conformados por reglas. La lógica del sistema seguirá esa estructura, por lo que el usuario deberá cargar las políticas al sistema a través de un archivo en formato *Source Data Stream* (*-ds.xml) y el sistema se encargará de obtener los perfiles y reglas como se muestra en el siguiente diagrama.

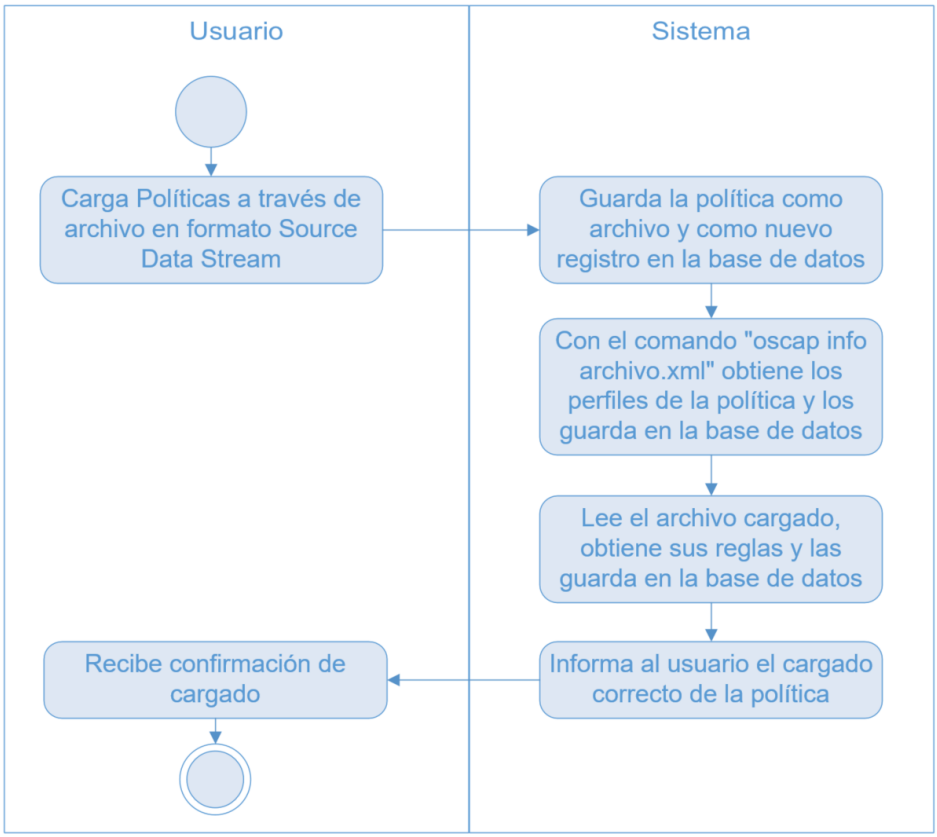


Figura 17: Diagrama de actividades de cargado de políticas
Fuente: Elaboración propia

Una vez cargada la política, el usuario puede utilizar uno de los perfiles por defecto para escanear y hardenizar un cliente o puede crear un nuevo perfil en base a una política y agregar o eliminar las reglas del perfil personalizado siguiendo el siguiente flujo.

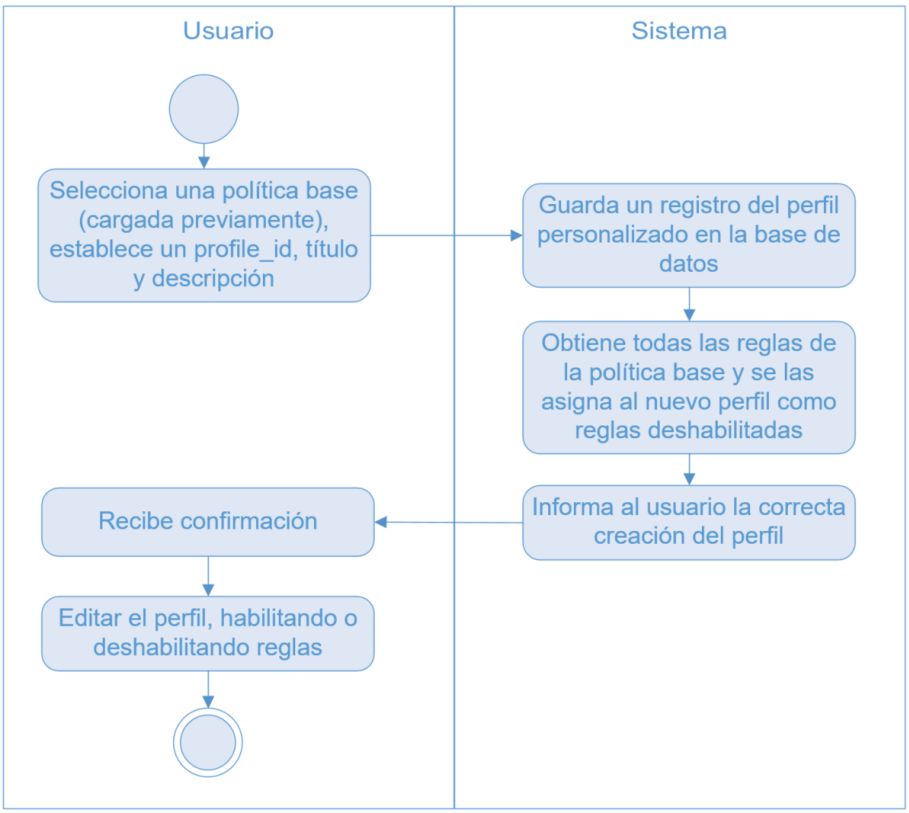


Figura 18: Diagrama de actividades de personalización de perfil
Fuente: Elaboración propia

Una vez creado el perfil, la habilitación / deshabilitación de reglas lo puede realizar el usuario en cualquier momento.

4.1.2. Gestión de Clientes

En el sistema se denomina “cliente” a todo dispositivo de cómputo que es objeto principal del proceso de hardening; si bien en el presente trabajo solo se evaluarán y hardenizarán servidores Ubuntu Linux, el sistema está preparado para operar con cualquier servidor que pueda ser administrado haciendo uso del protocolo de administración remota *SSH (Secure Shell)*.

La gestión de clientes permite agregar y modificar servidores, para lo cual el usuario deberá introducir los siguientes datos del cliente a agregar: nombre, descripción, dirección IPv4 y opcionalmente podrá guardar el usuario

y contraseña; si bien estos dos últimos campos son almacenados cifrados en la base de datos, es decisión del usuario final llenar estos campos o mantenerlos en blanco e introducir las credenciales únicamente cuando se ejecuta el escaneo y hardening, para evitar almacenar datos sensibles en la base de datos del sistema. Adicionalmente, durante la creación o modificación del cliente, el usuario final debe asignarle uno o varios perfiles contenidos en una de las políticas cargadas previamente.

4.1.3. Ejecución de Escaneo y Revisión de Resultados

Una vez que se creó el cliente y se le asignó un perfil, el administrador podrá realizar los escaneos simplemente pulsando un botón y el sistema se encargará del resto realizando las siguientes actividades.

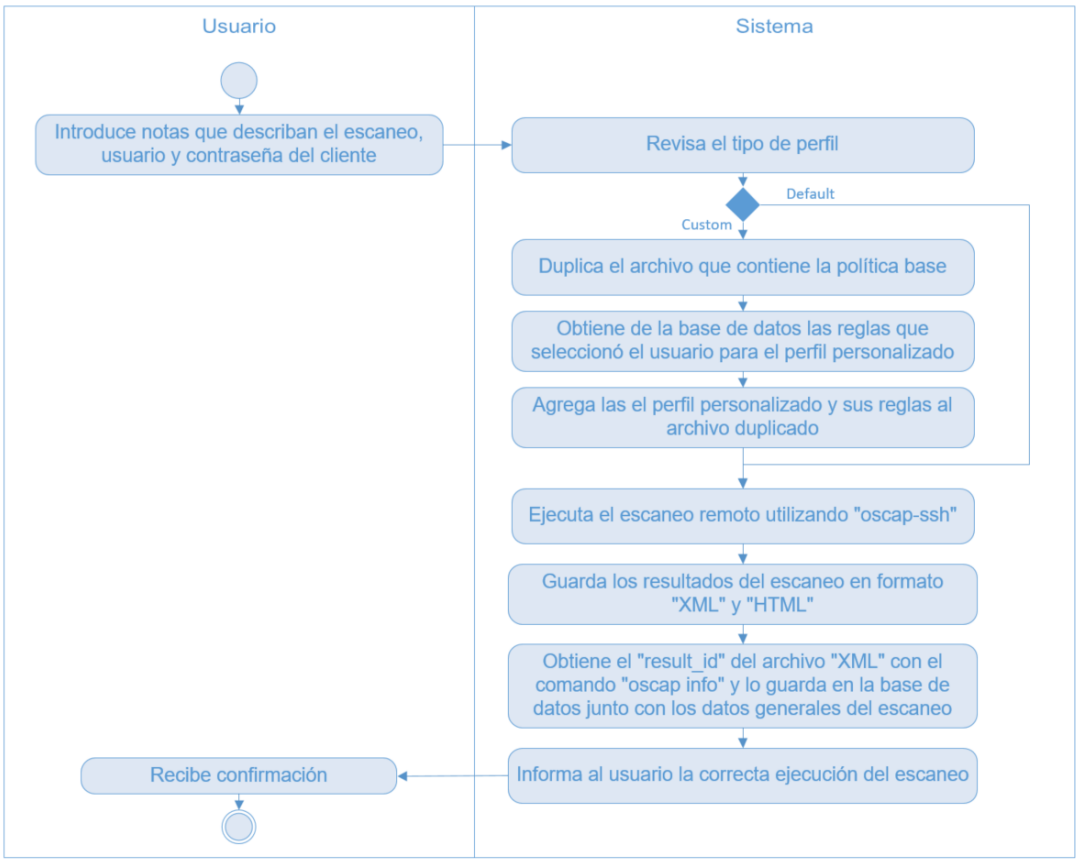


Figura 19: Diagrama de actividades de ejecución de escaneo
Fuente: Elaboración propia

Tras ejecutar el escaneo, el usuario puede revisar los resultados a través de un visor integrado en el sistema, del archivo en formato HTML generado por OpenSCAP.

4.1.4. Ejecución de Hardening y Revisión de Resultados

Finalmente, el último paso del proceso de hardening es precisamente la ejecución remota de configuraciones que hardenicen el sistema objetivo, para lo cual el usuario nuevamente debe limitarse únicamente a pulsar un botón y el sistema realiza las siguientes actividades.

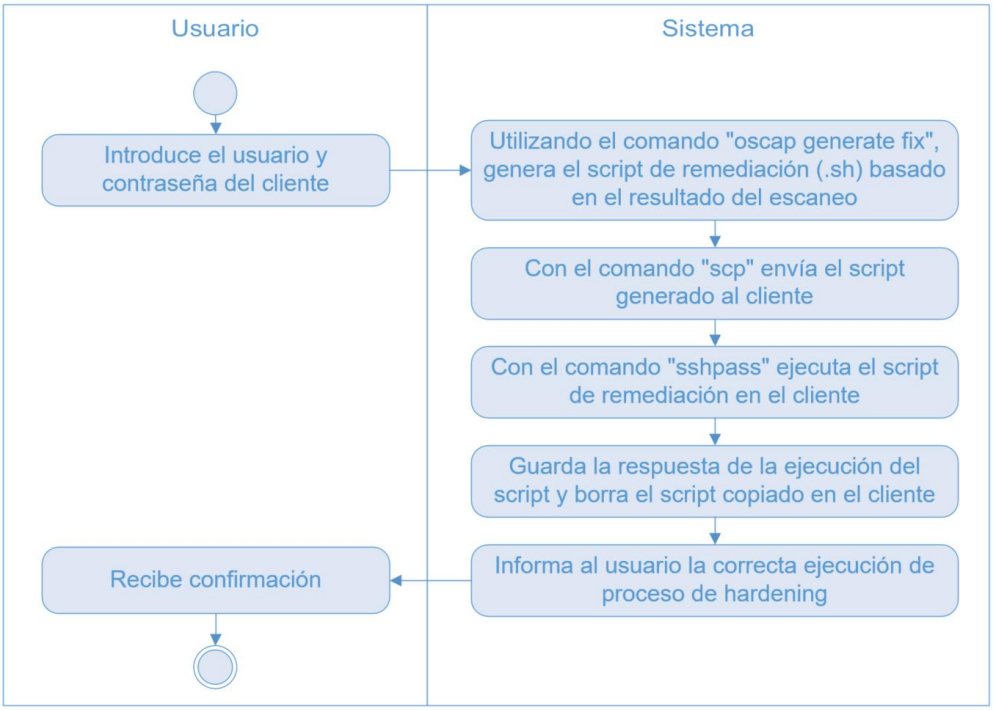


Figura 20: Diagrama de actividades de ejecución de hardening
Fuente: Elaboración propia

Tras ejecutar el hardening remotamente, el usuario puede revisar el resultado de la ejecución del script y si desea, descargarlo para su aplicación local, en otros servidores de manera masiva o cualquier otra actividad que el administrador considere necesaria.

4.1.5. Estructura de la Base de Datos

La estructura de la base de datos y los campos de las tablas se encuentran detallados en el Anexo A “Diagrama Relacional de la Base de Datos”.

4.2. Tecnologías Utilizadas

El sistema web propuesto emplea las siguientes tecnologías:

- Lenguaje de Programación: PHP

- Framework: Laravel
- Sistema de Administración de Base de Datos: MySQL
- Servidor Web: Apache
- Sistema Operativo: Ubuntu Server
- Herramienta base para evaluar los sistemas: *Open Security Content Automation Protocol* (oscap y oscap-ssh)
- Protocolo y librería para la difusión de scripts de hardenización: ssh y sshpass
- Adicionalmente, se hizo mucho uso de la interfaz de línea de comandos de Linux "*Bash"* y la librería "expect" para la generación y difusión de *scripts*

4.3. Desarrollo y Pruebas del Sistema

Todo el desarrollo sigue la filosofía de Open Source, por lo que el sistema puede ser descargado, revisado, modificado, utilizado y difundido por cualquier persona interesada. El código fuente se encuentra disponible en el repositorio público de GitHub "fabriciotorrico/UBA-MSI-TFM-Hardening"[4] y los paquetes a instalar para el correcto funcionamiento del sistema se encuentran en el Anexo B "Puesta en Operación del Sistema de Hardening".

Así mismo, si bien todo el proceso de hardening se lo realiza desde la interfaz de gráfica del sistema, el usuario final (administrador de infraestructura) debe asegurarse que el cliente pueda ser administrado vía *ssh* y tener instalado el paquete *oscap*. Los pasos a seguir en clientes con sistema operativo Ubuntu Linux son descritos en el Anexo C "Validaciones de Conectividad e Instalación de Paquetes en Clientes".

Una vez desarrollado e implementado el sistema y validada la conectividad con los clientes, se muestra a continuación el proceso de hardening completo que sería llevado a cabo por un administrador de infraestructura y sistemas.

[4] https://github.com/fabriciotorrico/UBA-MSI-TFM-Hardening

4.3.1. Acceso al Sistema

El acceso al sistema debe ser a través de un navegador web, con la dirección IP / *hostname* y las credenciales de acceso asignadas por el administrador.

Figura 21: Inicio de sesión para acceso al sistema
Fuente: Elaboración propia

Una vez digitado el usuario y contraseña correctos, se tiene acceso al sistema, donde están disponibles las siguientes secciones.

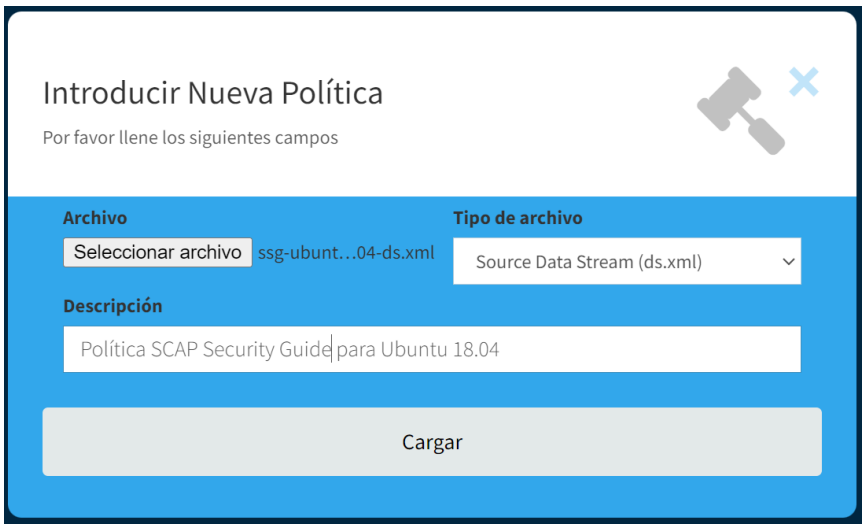
Figura 22: Detalle de secciones del sistema
Fuente: Elaboración propia

- En la sección 1 se encuentra el menú principal, a través del cual se acceden a las diferentes funcionalidades del sistema.
- La sección 2 es la superficie donde se interactuará con los distintos módulos del sistema.
- La sección 3 despliega un cuadro emergente que permite editar los datos personales, usuario y contraseña.

4.3.2. Políticas, Perfiles y Reglas

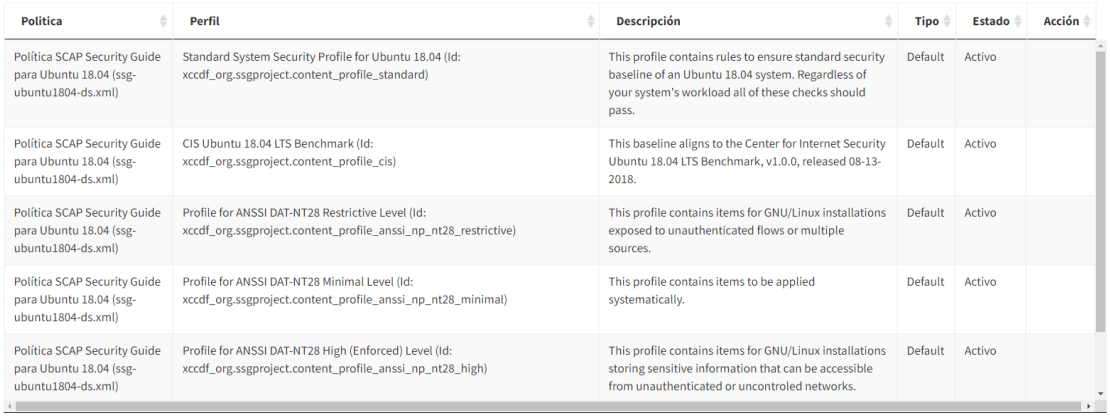
El primer paso tras acceder al sistema es agregar una política, para lo cual se debe acceder a “Políticas, perfiles y reglas” del menú principal y pulsar el botón “Cargar Nueva Política”.

Llenar los campos y subir el archivo en formato Source Data Stream.



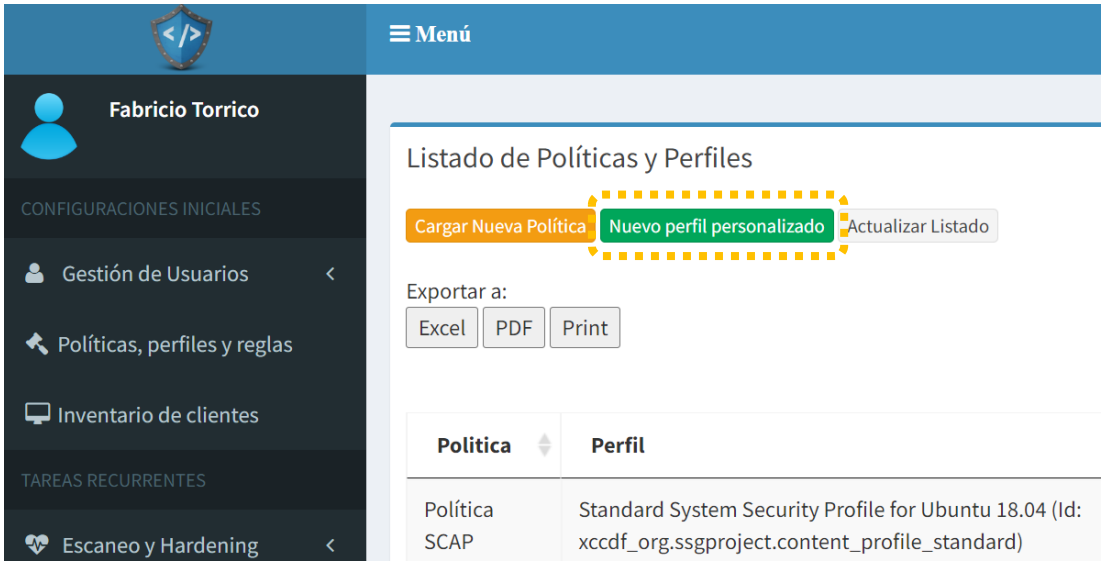
Si la política es cargada correctamente emergerá el siguiente aviso en la esquina inferior derecha.

Y en la tabla aparecerán los distintos perfiles contenidos en la política cargada.

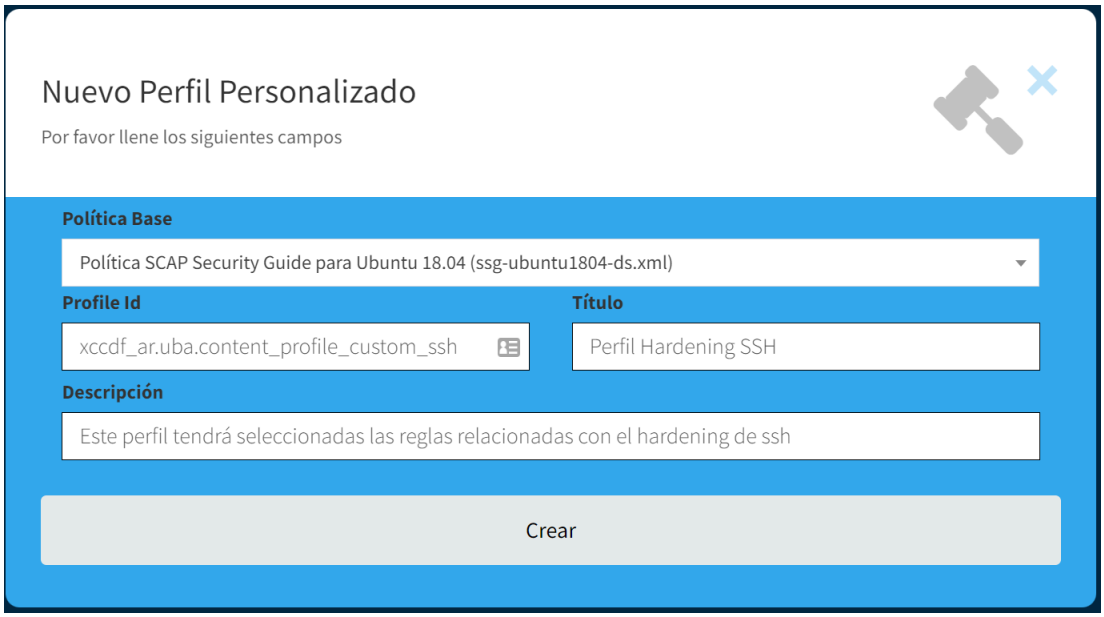


Politica	Perfil	Descripción	Tipo	Estado	Acción
Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Standard System Security Profile for Ubuntu 18.04 (Id: xccdf_org.ssgproject.content_profile_standard)	This profile contains rules to ensure standard security baseline of an Ubuntu 18.04 system. Regardless of your system's workload all of these checks should pass.	Default	Activo	
Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	CIS Ubuntu 18.04 LTS Benchmark (Id: xccdf_org.ssgproject.content_profile_cis)	This baseline aligns to the Center for Internet Security Ubuntu 18.04 LTS Benchmark, v1.0.0, released 08-13-2018.	Default	Activo	
Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	This profile contains items for GNU/Linux installations exposed to unauthenticated flows or multiple sources.	Default	Activo	
Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Minimal Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)	This profile contains items to be applied systematically.	Default	Activo	
Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)	This profile contains items for GNU/Linux installations storing sensitive information that can be accessible from unauthenticated or uncontroled networks.	Default	Activo	

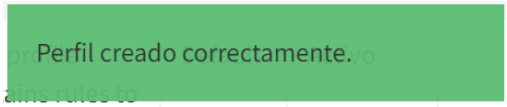
Cada uno de los perfiles cargados serán de tipo “Default” y puede ser asociado a un cliente pasa su escaneo y hardening. Sin embargo; con el objetivo de mostrar todas las funcionalidades del sistema, se creará un perfil personalizado y se seleccionarán algunas reglas. Para ello se debe pulsar el botón “Nuevo perfil personalizado”.



Llenar los campos del formulario y pulsar “Crear”.

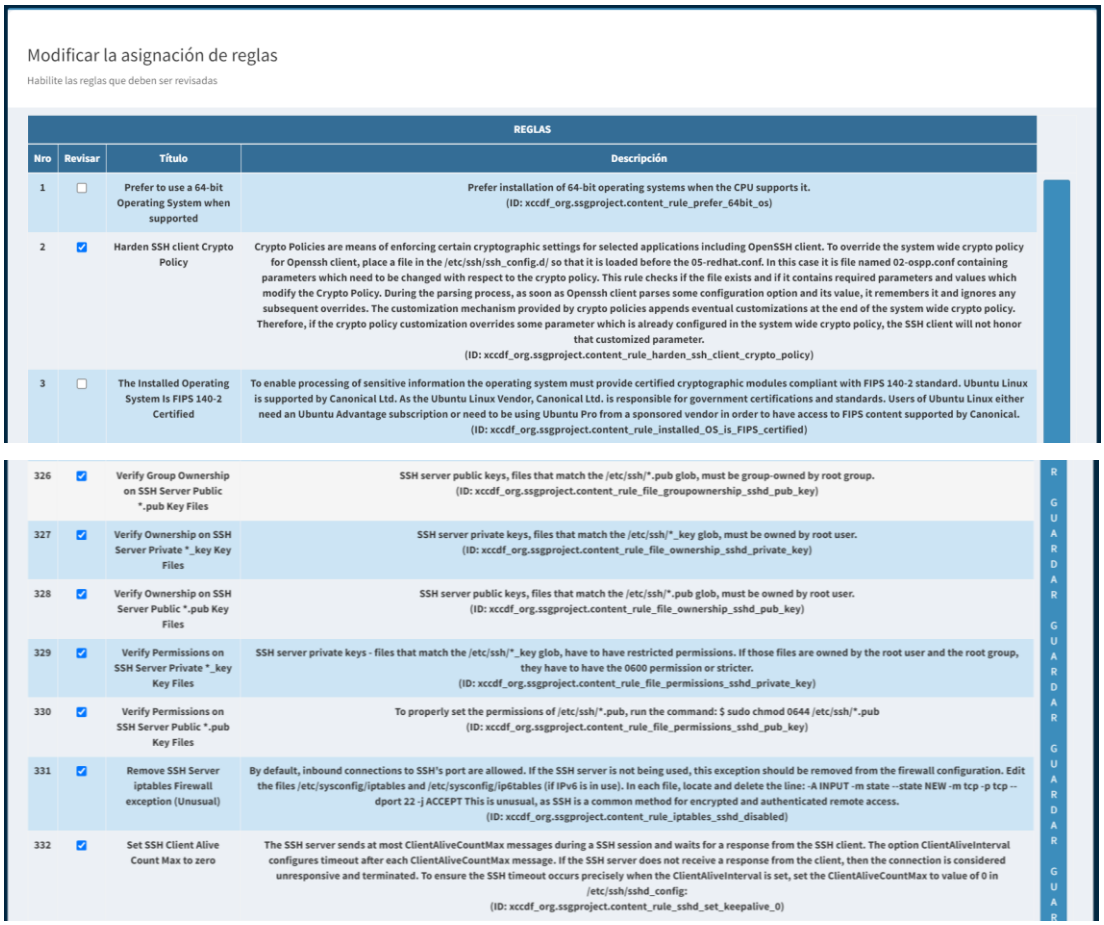


De manera similar al cargado de política y cualquier otra acción realizada en el sistema, tras su ejecución correcta emergerá un mensaje temporal en la esquina inferior derecha.



Y el perfil creado será cargado en la tabla de perfiles, donde se deberá pulsar el botón “Editar Reglas”.

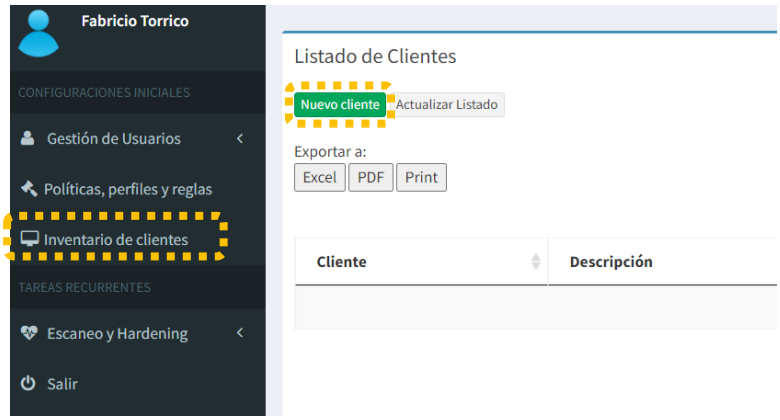
Como se evidencia, solo se pueden editar los perfiles de tipo “Custom” y no así los de tipo “Default” que fueron cargados junto con la política. Tras ingresar a la edición de reglas, se debe seleccionar (marcar el check) de todas aquellas reglas que se desea sean escaneadas y remediadas en el proceso de hardening.



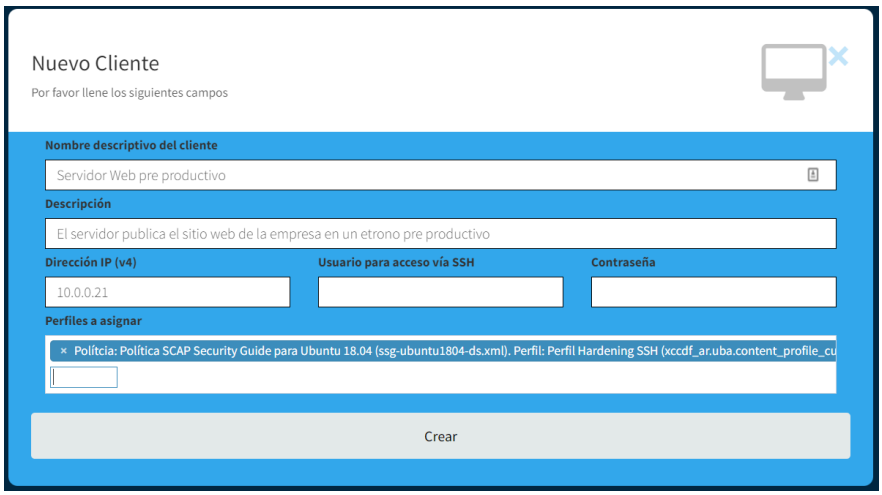
Para el presente ejemplo se seleccionarán las reglas relacionadas con SSH; una vez finalizada la selección, se debe pulsar el botón “Guardar” de la parte lateral derecha para confirmar la selección de reglas y cerrar la ventana emergente.

4.3.3. Inventario de Clientes

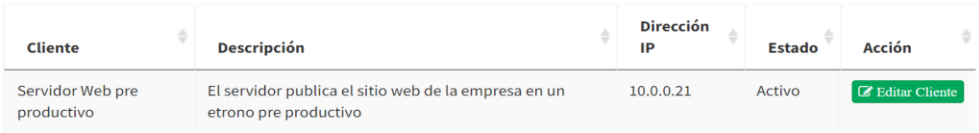
En el inventario de clientes se agregarán aquellos dispositivos de cómputo que se desea escanear y hardenizar, para ello se debe seleccionar “Inventario de Clientes” del menú principal y pulsar el botón “Nuevo Cliente”.



Llenar los campos del formulario y pulsar “Crear”. Como se detalló en el diseño del sistema, los campos “Usuario” y “Contraseña” no son obligatorios y la decisión de llenarlos es del administrador. Para el ejemplo se seleccionará el perfil creado en el punto previo; pero en una implementación real se pueden asociar tantos perfiles como el administrador considere necesario.



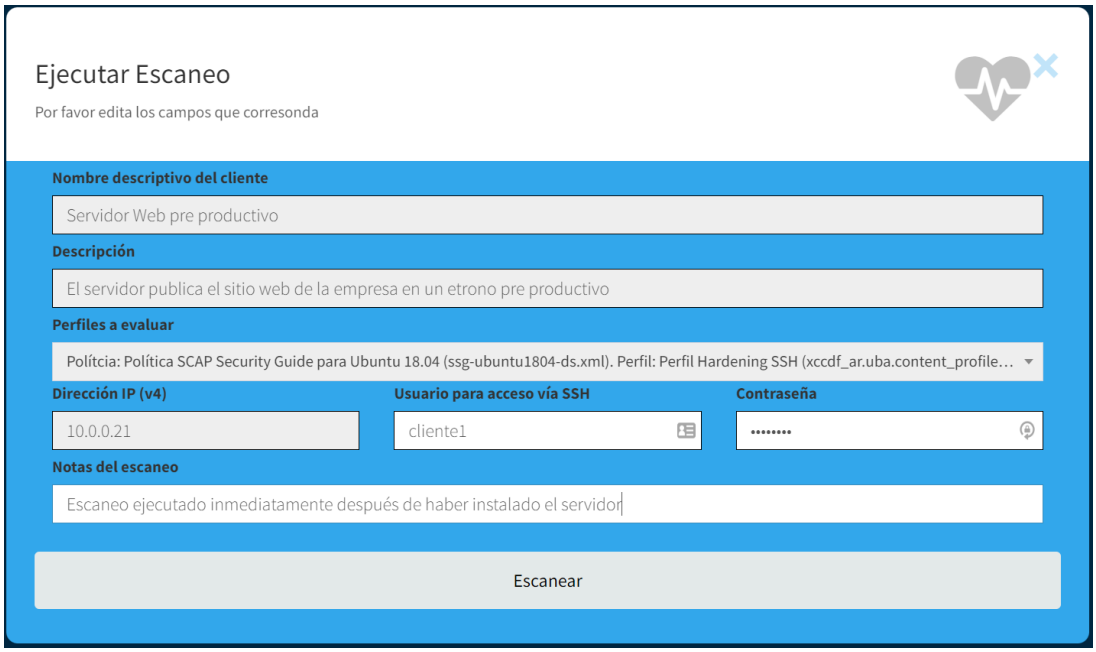
Nuevamente aparecerá el mensaje de creación exitosa y el cliente formará parte del inventario de clientes.



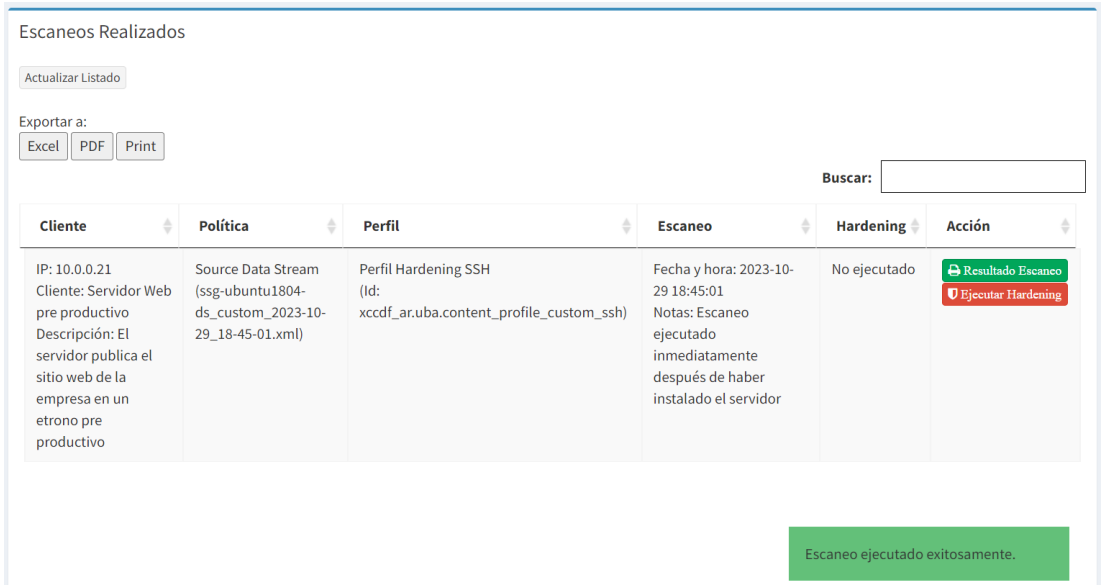
4.3.4. Escanear

Tras agregar al cliente y asociar una política, ejecutar el escaneo será tan sencillo como seleccionar “Escanear” del menú principal y pulsar el botón “Escanear” del listado de clientes / políticas disponibles.

Llenar los campos del formulario, que además estarán llenos en caso de que el administrador haya decidido almacenar las credenciales en la base de datos del sistema y pulsar escanear.



El sistema ejecutará el escaneo y si el proceso se ejecuta correctamente dirigirá al usuario al módulo “Resultados y Hardening”, mostrando el mensaje de éxito.



En el listado de escaneos realizados se podrá imprimir el resultado pulsando el botón “Resultado Escaneo”, que despegará una ventana emergente con el Reporte de Evaluación OpenSCAP.

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Ubuntu 18.04

with profile Perfil Hardening SSH

— Este perfil tendrá seleccionadas las reglas relacionadas con el hardening de ssh

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 Ubuntu 18.04. 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.

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.

Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.oRu081lHhk/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_ar.uba.content_profile_custom_ssh
Started at	2023-10-29T22:45:03
Finished at	2023-10-29T22:45:03
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4	127.0.0.1
IPv4	10.0.0.21
IPv4	192.168.1.203
IPv6	0:0:0:0:0:0:0:1
IPv6	fe80:0:0:0:a00:27ff:fe45:343
IPv6	fe80:0:0:0:a00:27ff:fe11:70bc
MAC	00:00:00:00:00:00
MAC	08:00:27:45:03:43
MAC	08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 4 rules! Please review rule results and consider applying remediation.

Rule results

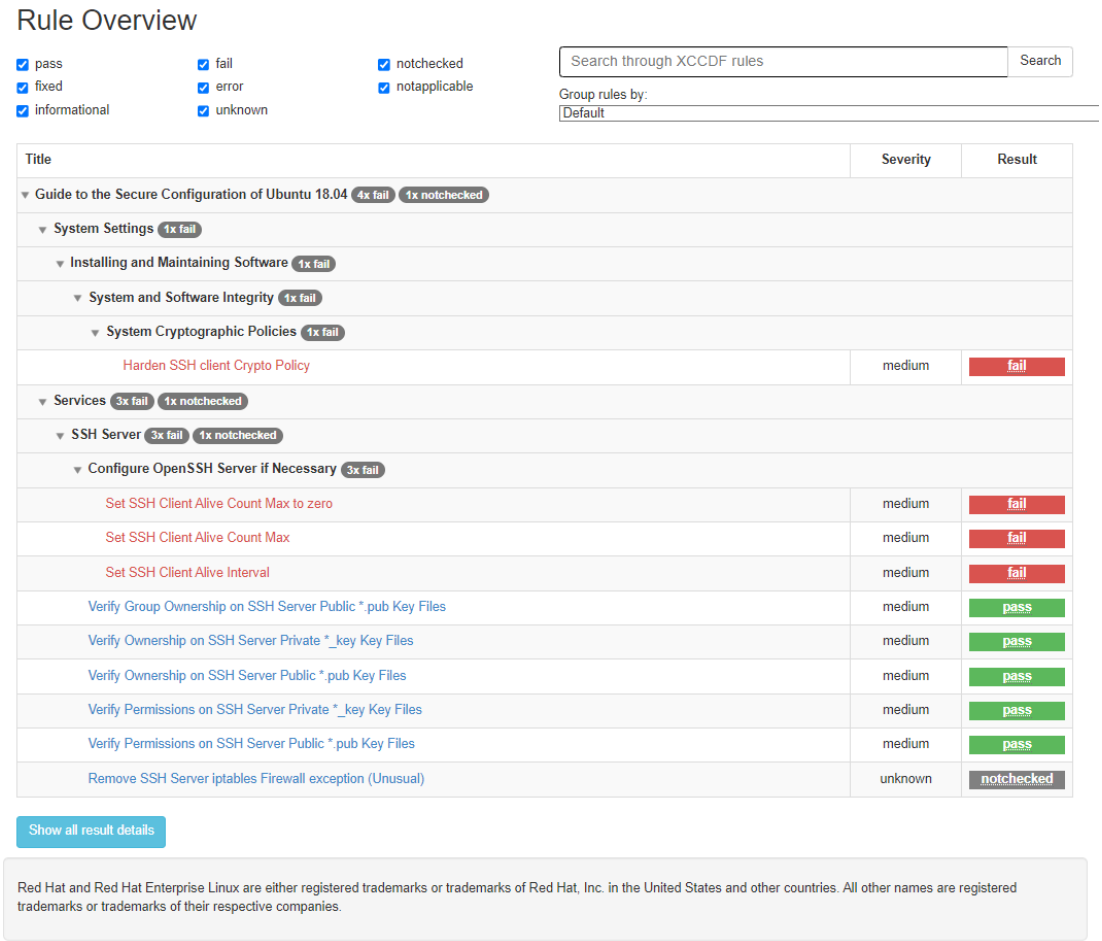
5 passed | 4 failed | 1 other

Severity of failed rules

4 medium

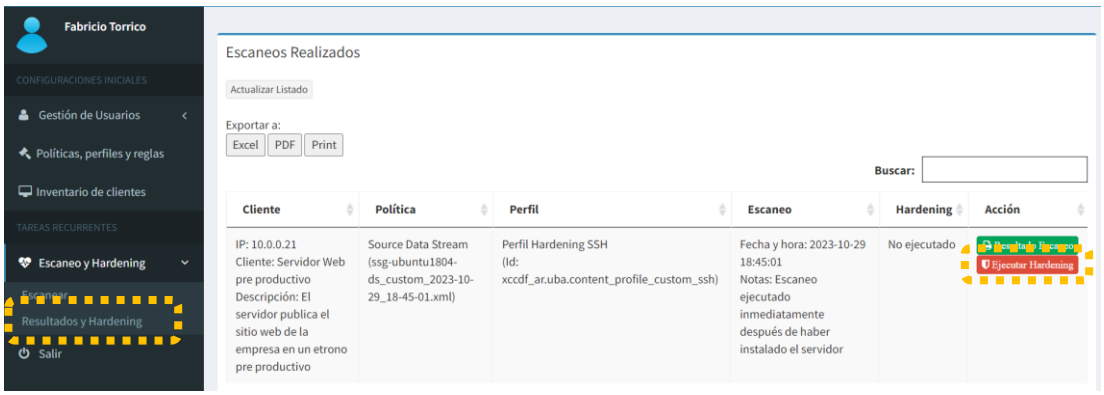
Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	41.666668	100.000000	41.67%



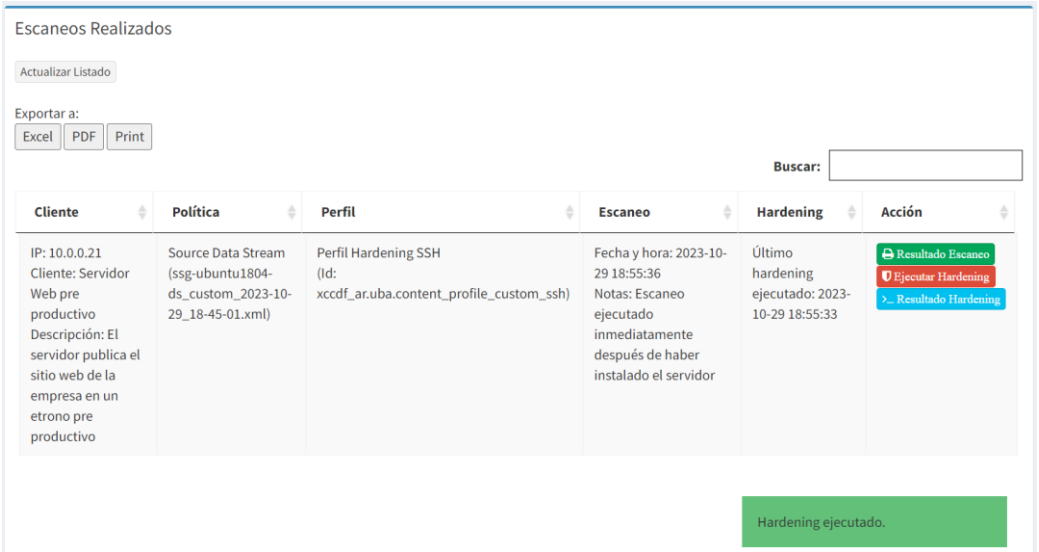
4.3.5. Resultados y Hardening

Finalmente, para ejecutar el Hardening en el cliente se debe ingresar a “Resultados y Hardening” del menú principal y pulsar el botón “Ejecutar Hardening”.

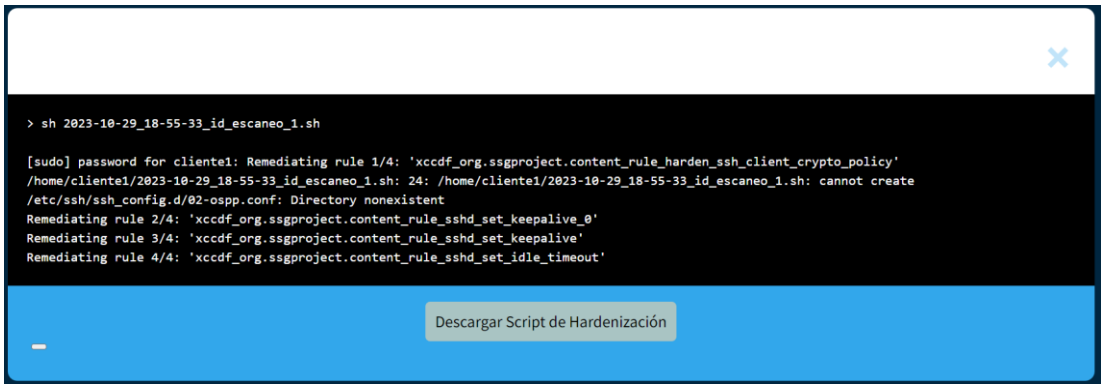


De manera similar al proceso de escaneo, el cliente debe introducir las credenciales, pulsar el botón “Ejecutar tareas de hardenización” y el sistema hará el resto.

Si todo el proceso se ejecuta correctamente, se mostrará el mensaje de éxito y un botón adicional de “Resultado Hardening”.



Pulsando el botón “Resultado Hardening” se puede visualizar el resultado de la ejecución del script de hardenización en el cliente y si se desea, descargar el script ejecutado.



Con eso concluiría una primera vuelta del proceso de hardening del servidor; que al ser un proceso de mejora continua, muy probablemente el administrador aplicará más perfiles o agregará reglas a un perfil personalizado y ejecutará reiteradas veces el escaneo y hardenización; lo cual será tan simple como pulsar dos botones para cada acción y revisar los resultados.

5. VALIDACIÓN DE HIPÓTESIS

La hipótesis del presente trabajo plantea que el sistema desarrollado mejora los niveles de seguridad de los servidores en los que se ejecuta. Para validar la hipótesis se agregó al "Sistema de Hardening Centralizado" desarrollado en el presente trabajo, la política "ssg-ubuntu1804-ds.xml"[5], se asociaron los perfiles por defecto contenidos en la política a un cliente Ubuntu Server 18.04 recién instalado y se ejecutaron escaneos antes y después de la ejecución del proceso de hardening.

Con la ejecución de hardening y la revisión de resultados obtenidos se evidenció que si bien las reglas "aprobadas" (aplicadas exitosamente) incrementaron (marcadas en amarillo en la siguiente tabla); los *scripts* contenidos en la política y que permiten hardenizar el cliente se ejecutan de manera secuencial, por lo que una falla durante la remediación de una regla generará que el script se deje de ejecutar, por lo que se decidió descargar los scripts a través disponible en el sistema, eliminar los elementos que generan conflictos y ejecutarlos nuevamente, lo cual mejoró aún más los resultados obtenidos (marcados en verde en la siguiente tabla); los cuales también son considerados válidos para la validación de hipótesis tomando en cuenta que estas inconsistencias no son errores del sistema desarrollado sino de la política de *SCAP Security Guide* utilizada; tomando en cuenta además que el sistema considera este aspecto y permite la descarga del script para que el administrador del sistema pueda controlar estos elementos detectados.

Se evaluaron 5 perfiles de la política y se promedió la mejora porcentual de aquellos perfiles que experimentaron mejoras tras la ejecución del proceso de hardening. Los resultados obtenidos son plasmados en la siguiente tabla

Perfil	Escaneo antes del hardening			Escaneo después del hardening			Mejora porcentual	Escaneo después del hardening modificando			Mejora porcentual
	Aprobadas	Fallidas	Errores	Aprobadas	Fallidas	Errores		Aprobadas	Fallidas	Errores	
Profile for ANSSI DAT-NT28 Average (Intermediate) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average)	21	15	4	21	15	4	0,00%	27	9	4	28,57%
Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)	23	17	4	26	15	4	13,04%	32	9	4	39,13%
Profile for ANSSI DAT-NT28 Minimal Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)	17	0	2	17	0	2	0,00%	17	0	2	0,00%
Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	23	16	4	25	15	4	8,70%	31	9	4	34,78%
Standard System Security Profile for Ubuntu 18.04 (Id: xccdf_org.ssgproject.content_profile_standard)	25	16	2	27	15	2	8,00%	33	9	2	32,00%
							9,91%				33,62%

[5] https://static.open-scap.org/ssg-guides/ssg-ubuntu1804-guide-index.html

El Anexo D contiene el detalle de las pruebas de validación de hipótesis y como se evidencia en los resultados de la tabla previa, se concluye que el sistema desarrollado mejora los niveles de seguridad de los servidores en los que se ejecuta en promedio en un 9.91% utilizando el sistema sin ningún cambio y en un 33.62% modificando los scripts de hardenización contenidos en las políticas cargadas al sistema, validando de ese modo la hipótesis planteada.

CONCLUSIONES

Tras haber investigado en profundidad diferentes guías y estándares emitidos por organizaciones, comunidades y entidades gubernamentales reconocidas mundialmente como lo son CIS (Center for Internet Security), NIST, SANS, DISA, entre otras; se evidenció que si bien todas ellas desarrollan lineamientos para el proceso de hardening, en general buscan la estandarización del proceso y todo parece apuntar a que el estándar SCAP (Security Content Automation Protocol) desarrollado por el NIST será (si es que no lo es ya) el lineamiento base para todo proceso de hardening automatizado. Tras revisar los lineamientos emitidos por estas organizaciones, se revisaron herramientas de código abierto como lo son Bastille Linux, Lynis y Ubuntu Security Guide, además de distintos repositorios en GitHub que contienen herramientas y scripts para hardenizar servicios. Finalmente, se analizaron soluciones de paga que apoyan en el proceso de hardening como lo son CalCom Hardening Solution (que trabaja con agentes), ConfigOS Command Center (que trabaja sin agentes) y Runecast Analyzer (que puede trabajar de manera híbrida); todas las soluciones fueron evaluadas en versiones demo o a través de reuniones con el fabricante.

Tras contar con los insumos detallados en el párrafo previo, se evidenció que utilizar las herramientas proporcionadas por OpenSCAP para la aplicación de los estándares SCAP es la mejor alternativa libre a tomar como base para el desarrollo de un sistema que apoyará en el proceso de automatización de hardening de manera centralizada. Al evidenciar aquello, se procedió con el desarrollo de un sistema web que en términos generales brinda al usuario final una herramienta gráfica done puede cargar políticas en formato “Source Data Stream” (XML) que son desarrolladas y puestas a disposición de manera gratuita por diversas organizaciones, asociar los perfiles contenidos en las políticas con los “clientes” que desea hardenizar y a través del protocolo SSH ejecutar escaneos y hardening de manera remota.

Sin lugar a dudas el sistema desarrollado facilita y agiliza el proceso de hardening ya que el administrador (una vez cargadas las políticas y los

clientes), puede ejecutar escaneos y hardening pulsando únicamente dos botones y teniendo a disposición los resultados de ambas tareas. Adicionalmente, se demostró cuantitativamente la hipótesis planteada, evidenciando que únicamente con el uso del sistema desarrollado la seguridad de los servidores incrementa en promedio en un 10% y si adicionalmente el administrador descarga los scripts de hardening, omite las reglas que generan problemas y los ejecuta nuevamente, las mejoras de seguridad incrementan en promedio en un 34%.

Finalmente, a modo de recomendación se plantea que si bien la versión 1 del sistema desarrollado cumple el objetivo planteado en el presente trabajo, durante la investigación y desarrollo se evidenció que existen elementos adicionales que podrían agregar valor en futuras versiones del sistema, por lo que el autor insta a cualquier persona interesada en dar continuidad al presente trabajo a descargarlo de manera libre del repositorio GitHub y trabajar en mejoras como la implementación de agentes que permita obtener información más detallada de los clientes; el desarrollo de módulos que permitan al sistema realizar *rollback* de configuraciones; módulos que permitan la configuración de tareas de escaneo y hardening programadas; si bien la versión actual del sistema permite hardenizar cualquier servidor Linux que pueda ser accedido y administrado a través del protocolo SSH, para versiones posteriores sería interesante implementar módulos para hardenizar servidores Windows; proponer un entrono colaborativo conformando una comunidad donde sus integrantes puedan subir políticas, perfiles y reglas que serán puntuadas, generando un ranking de las mejores reglas; estas y muchas otras mejoras pueden ser desarrolladas para futuras versiones del sistema, por lo que se concluye además que el trabajo realizado no es una simple una herramienta más de hardenización, sino que tiene expectativas de crecimiento muy amplias.

GLOSARIO

Dirección IP : Dirección única que identifica a un dispositivo en Internet o en una red local.

Hostname : Nombre único que se le da a un dispositivo conectado a una red informática.

Navegador web : Software, aplicación o programa que permite el acceso a la web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser vistos.

Script : Archivo contiene una secuencia de comandos e instrucciones a ser ejecutadas por una computadora.

SSH : Protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

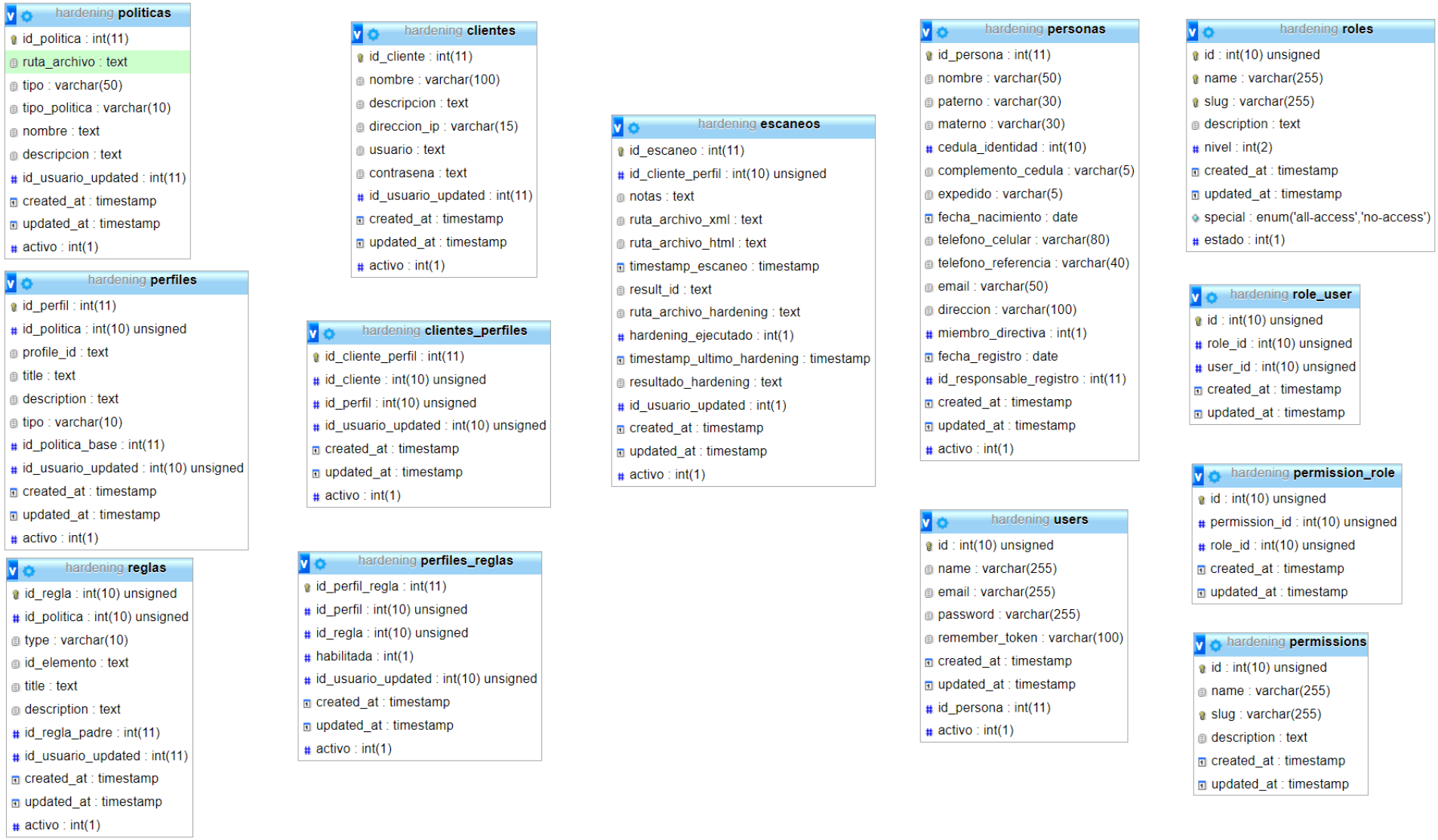
Terminal : Software o dispositivo electrónico que se emplea para interactuar con un computador.

Vulnerabilidad : Falla que permite que una amenaza se convierta en un riesgo.

ANEXOS

ANEXO A

Diagrama Relacional de la Base de Datos


hardening politicas
id_politica : int(11)
ruta_archivo : text
tipo : varchar(50)
tipo_politica : varchar(10)
nombre : text
descripcion : text
id_usuario_updated : int(11)
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening perfiles
id_perfil : int(11)
id_politica : int(10) unsigned
profile_id : text
title : text
description : text
tipo : varchar(10)
id_politica_base : int(11)
id_usuario_updated : int(10) unsigned
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening reglas
id_regla : int(10) unsigned
id_politica : int(10) unsigned
type : varchar(10)
id_elemento : text
title : text
description : text
id_regla_padre : int(11)
id_usuario_updated : int(11)
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening clientes
id_cliente : int(11)
nombre : varchar(100)
descripcion : text
direccion_ip : varchar(15)
usuario : text
contrasena : text
id_usuario_updated : int(11)
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening clientes_perfiles
id_cliente_perfil : int(11)
id_cliente : int(10) unsigned
id_perfil : int(10) unsigned
id_usuario_updated : int(10) unsigned
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening perfiles_reglas
id_perfil_regla : int(11)
id_perfil : int(10) unsigned
id_regla : int(10) unsigned
habilitada : int(1)
id_usuario_updated : int(10) unsigned
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening escaneos
id_escaneo : int(11)
id_cliente_perfil : int(10) unsigned
notas : text
ruta_archivo_xml : text
ruta_archivo_html : text
timestamp_escaneo : timestamp
result_id : text
ruta_archivo_hardening : text
hardening_ejecutado : int(1)
timestamp_ultimo_hardening : timestamp
resultado_hardening : text
id_usuario_updated : int(1)
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening personas
id_persona : int(11)
nombre : varchar(50)
paterno : varchar(30)
materno : varchar(30)
cedula_identidad : int(10)
complemento_cedula : varchar(5)
expedido : varchar(5)
fecha_nacimiento : date
telefono_celular : varchar(80)
telefono_referencia : varchar(40)
email : varchar(50)
direccion : varchar(100)
miembro_directiva : int(1)
fecha_registro : date
id_responsable_registro : int(11)
created_at : timestamp
updated_at : timestamp
activo : int(1)
hardening users
id : int(10) unsigned
name : varchar(255)
email : varchar(255)
password : varchar(255)
remember_token : varchar(100)
created_at : timestamp
updated_at : timestamp
id_persona : int(11)
activo : int(1)
hardening roles
id : int(10) unsigned
name : varchar(255)
slug : varchar(255)
description : text
nivel : int(2)
created_at : timestamp
updated_at : timestamp
special : enum('all-access','no-access')
estado : int(1)
hardening role_user
id : int(10) unsigned
role_id : int(10) unsigned
user_id : int(10) unsigned
created_at : timestamp
updated_at : timestamp
hardening permission_role
id : int(10) unsigned
permission_id : int(10) unsigned
role_id : int(10) unsigned
created_at : timestamp
updated_at : timestamp
hardening permissions
id : int(10) unsigned
name : varchar(255)
slug : varchar(255)
description : text
created_at : timestamp
updated_at : timestamp

ANEXO B

Puesta en Operación del Sistema de Hardening

Detalles del del servidor web que publica el sistema

VM: Ubuntu18.04-UBA-TFM

Usuario: fabri

Contraseña: fabri

Dirección IP: 10.0.0.10

Sistema Operativo: Ubuntu 18.04

Instalación de OpenSCAP

$ apt-get install libopenscap8

```
fabri@fabri-VirtualBox:~$ sudo su
[sudo] password for fabri:
root@fabri-VirtualBox:/home/fabri# apt-get install libopenscap8
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libopenscap8
0 upgraded, 1 newly installed, 0 to remove and 358 not upgraded.
Need to get 2.438 kB of archives.
After this operation, 65,6 MB of additional disk space will be used.
Get:1 http://bo.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 libopenscap8 amd64 1.2.15-1ubuntu0.4 [2.438 kB]
Fetched 2.438 kB in 2s (1.379 kB/s)
Selecting previously unselected package libopenscap8.
(Reading database ... 205863 files and directories currently installed.)
Preparing to unpack .../libopenscap8_1.2.15-1ubuntu0.4_amd64.deb ...
Unpacking libopenscap8 (1.2.15-1ubuntu0.4) ...
Setting up libopenscap8 (1.2.15-1ubuntu0.4) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
root@fabri-VirtualBox:/home/fabri#
```

Descarga, compilación e instalación de SCAP Security Guide

$ git clone https://github.com/ComplianceAsCode/content.git

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# git clone https://github.com/ComplianceAsCode/content.git
Cloning into 'content'...
remote: Enumerating objects: 402751, done.
remote: Counting objects: 100% (30186/30186), done.
remote: Compressing objects: 100% (1884/1884), done.
remote: Total 402751 (delta 28792), reused 28501 (delta 28232), pack-reused 372565
Receiving objects: 100% (402751/402751), 85.58 MiB | 993.00 KiB/s, done.
Resolving deltas: 100% (264974/264974), done.
```

$ apt-get install cmake make expat libxml2-utils ninja-build python3-jinja2 python3-yaml xsltproc

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# apt-get install cmake make expat libopenscap8 libxml2-utils ninja-build python3-jinja2 python3-yaml xsltproc
Reading package lists... Done
Building dependency tree
Reading state information... Done
make is already the newest version (4.1-9.1ubuntu1).
make set to manually installed.
python3-yaml is already the newest version (3.12-1build2).
libopenscap8 is already the newest version (1.2.15-1ubuntu0.4).
The following additional packages will be installed:
  cmake-data libjsoncpp1 librhash0 libuv1
Suggested packages:
  cmake-doc python-jinja2-doc
The following NEW packages will be installed:
  cmake cmake-data expat libjsoncpp1 librhash0 libuv1 libxml2-utils ninja-build python3-jinja2 xsltproc
0 upgraded, 10 newly installed, 0 to remove and 358 not upgraded.
Need to get 4.953 kB of archives.
After this operation, 26,0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://bo.archive.ubuntu.com/ubuntu bionic-updates/main amd64 cmake-data all 3.10.2-1ubuntu2.18.04.2 [1.332 kB]
Get:2 http://bo.archive.ubuntu.com/ubuntu bionic/main amd64 libjsoncpp1 amd64 1.7.4-3 [73,6 kB]
Get:3 http://bo.archive.ubuntu.com/ubuntu bionic/main amd64 librhash0 amd64 1.3.6-2 [78,1 kB]
Get:4 http://bo.archive.ubuntu.com/ubuntu bionic/main amd64 libuv1 amd64 1.18.0-3 [64,4 kB]
Get:5 http://bo.archive.ubuntu.com/ubuntu bionic-updates/main amd64 cmake amd64 3.10.2-1ubuntu2.18.04.2 [3.152 kB]
Get:6 http://bo.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 expat amd64 2.2.5-3ubuntu0.9 [15,0 kB]
Get:7 http://bo.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libxml2-utils amd64 2.9.4+dfsg1-6.1ubuntu1.9 [35,9 kB]
Get:8 http://bo.archive.ubuntu.com/ubuntu bionic/universe amd64 ninja-build amd64 1.8.2-1 [93,3 kB]
Get:9 http://bo.archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-jinja2 all 2.10-1ubuntu0.18.04.1 [95,4 kB]
Get:10 http://bo.archive.ubuntu.com/ubuntu bionic-updates/main amd64 xsltproc amd64 1.1.29-5ubuntu0.3 [14,0 kB]
Fetched 4.953 kB in 4s (1.340 kB/s)
```

$ cd content

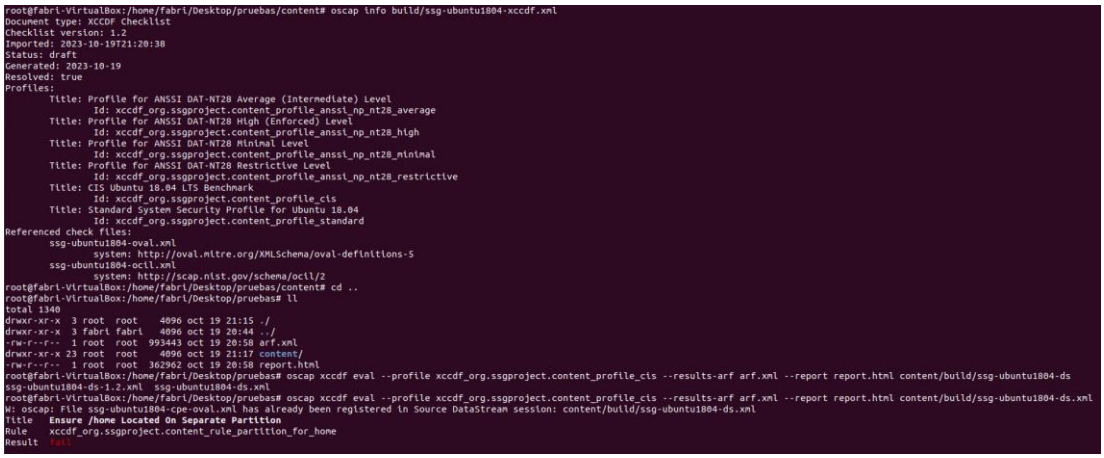
$ ./build_product ubuntu1804

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas/content# ./build_product ubuntu1804
-- SCAP Security Guide 0.1.71
-- (see /home/fabri/Desktop/pruebas/content/docs/manual/developer_guide.adoc for build instructions)
--
-- Found PythonInterp: /usr/bin/python3 (found version "3.6.9")
-- Found PY_yaml: /usr/lib/python3/dist-packages/yaml
-- Found PY_jinja2: /usr/lib/python3/dist-packages/jinja2
-- Could NOT find PY_lxml (missing: PY_LXML)
-- Could NOT find PY_pytest (missing: PY_PYTEST)
-- Could NOT find PY_pytest_cov (missing: PY_PYTEST_COV)
-- Could NOT find PY_json2html (missing: PY_JSON2HTML)
-- Could NOT find PY_mypy (missing: PY_MYPY)
-- Could NOT find PY_openpyxl (missing: PY_OPENPYXL)
-- Could NOT find PY_pandas (missing: PY_PANDAS)
-- Could NOT find PY_pcre2 (missing: PY_PCRE2)
-- Could NOT find PY_cmakelint (missing: PY_CMAKELINT)
-- Could NOT find PY_sphinx (missing: PY_SPHINX)
-- Could NOT find PY_sphinxcontrib.autojinja (missing: PY_SPHINXCONTRIB.AUTOJINJA)
-- Could NOT find PY_sphinx_rtd_theme (missing: PY_SPHINX_RTD_THEME)
-- Could NOT find PY_myst_parser (missing: PY_MYST_PARSER)
-- Could NOT find PY_prometheus_client (missing: PY_PROMETHEUS_CLIENT)
-- CMake:
```

Revisión de archivos y evaluación local

$ oscap info ssg-ubuntu1804-xccdf.xml

$ oscap xccdf eval --profile perfil_a_evaluar --results-arf resutlados_arf.xml --report reporte_html.html politica-ds.xml



Instalación de oscap-ssh

$ wget https://raw.githubusercontent.com/OpenSCAP/openscap/maint-1.2/utils/oscap-ssh

$ chmod 755 oscap-ssh

$ mv –v oscap-ssh /usr/local/bin

$ chown root:root /usr/local/bin/oscap-ssh

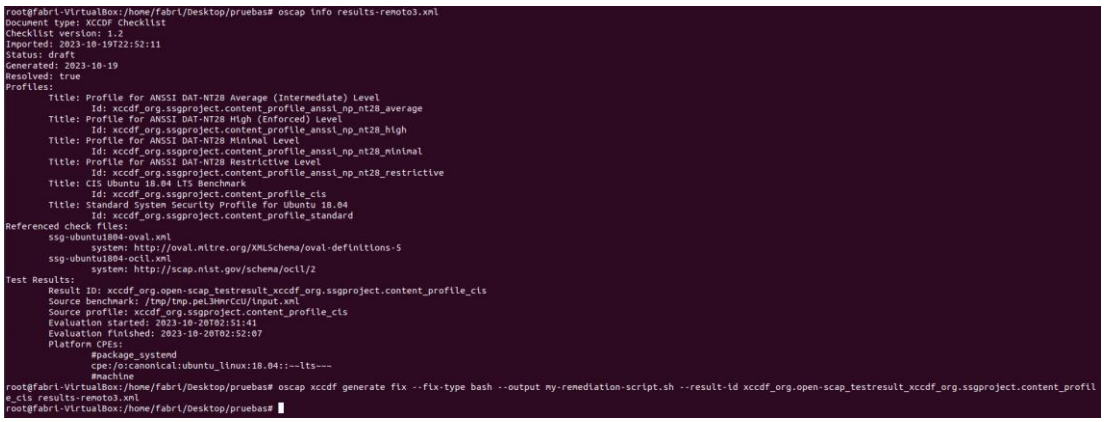
Evaluación remota

$ oscap-ssh nombre_usuario@direccion.ip.del.cliente xccdf eval --profile perfil_a_evaluar -- results resutlados.xml --report reporte_html.html politica-ds.xml

Generación de archivos de hardening (remediación) en base a resultados

$ oscap info resultados.xml //Para obtener el “Result ID”

$ oscap xccdf generate fix --fix-type bash --output script.sh --result-id Result_ID_obtenido resultados.xml



Copiado y ejecución remota de script

$ scp script.sh nombre_usuario@direccion.ip.del.cliente:/ruta/destino

$ ssh -t nombre_usuario@direccion.ip.del.cliente 'sudo sh /ruta/destino/script.sh'

Generación de script de todas las reglas de un perfil

$ oscap xccdf generate fix --profile perfil_deseado archive-ds.xml > script.sh

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# oscap xccdf generate fix --profile xccdf_org.ssgpr
oject.content_profile_cis content/build/ssg-ubuntu1804-ds.xml > script.sh
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# oscap xccdf generate fix --profile xccdf_org.ssgpr
oject.content_profile_cis content/build/ssg-ubuntu1804-xccdf.xml > script2.sh
```

Instalación del paquete “xmlstarlet” para la ejecución de scripts para obtención de ID de reglas

$ apt-get install xmlstarlet

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# apt-get install xmlstarlet
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  xmlstarlet
0 upgraded, 1 newly installed, 0 to remove and 358 not upgraded.
```

Instalación del paquete “expect” para la ejecución de oscap-ssh sin interacción humana

$ apt-get install expect

```
root@fabri-VirtualBox:/home/fabri# apt-get install expect
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-hwe-5.4-headers-5.4.0-132
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libtcl8.6 tcl-expect tcl8.6
Suggested packages:
  tk8.6 tcl-tclreadline
The following NEW packages will be installed:
  expect libtcl8.6 tcl-expect tcl8.6
0 upgraded, 4 newly installed, 0 to remove and 240 not upgraded.
Need to get 1.138 kB of archives.
After this operation, 4.598 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://bo.archive.ubuntu.com/ubuntu bionic/main amd64 libtcl8.6 amd64 8.6.8+dfsg-3 [881 kB]
Get:2 http://bo.archive.ubuntu.com/ubuntu bionic/universe amd64 tcl-expect amd64 5.45.4-1 [105 kB]
Get:3 http://bo.archive.ubuntu.com/ubuntu bionic/universe amd64 expect amd64 5.45.4-1 [137 kB]
```

Instalación del paquete “sshpass” para la enviar pasar la contraseña ssh como argumento del comando

$ apt-get install sshpass

```
root@fabri-VirtualBox:/var/www/html/hardening/public/oscap/scripts-remediacion# apt install sshpass
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  sshpass
0 upgraded, 1 newly installed, 0 to remove and 240 not upgraded.
Need to get 10,5 kB of archives.
After this operation, 30,7 kB of additional disk space will be used.
Get:1 http://bo.archive.ubuntu.com/ubuntu bionic/universe amd64 sshpass amd64 1.06-1 [10,5 kB]
Fetched 10,5 kB in 1s (8.458 B/s)
```

Instalación de SCAP Workbench (Opcional)

$ apt-get install scap-workbench

```
root@fabri-VirtualBox:/home/fabri/Desktop/pruebas# apt-get install scap-workbench
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libmng2 libmysqlclient20 libqt4-dbus libqt4-declarative libqt4-network libqt4-script libqt4-sql
  libqt4-sql-mysql libqt4-xml libqt4-xmlpatterns libqtcore4 libqtdbus4 libqtgui4 qdbus qt-at-spi
  qtchooser qtcore4-l10n ssh-askpass
Suggested packages:
  libqt4-declarative-folderlistmodel libqt4-declarative-gestures libqt4-declarative-particles
  libqt4-declarative-shaders qt4-qmlviewer libqt4-dev libicu55 qt4-qtconfig
The following NEW packages will be installed:
  libmng2 libmysqlclient20 libqt4-dbus libqt4-declarative libqt4-network libqt4-script libqt4-sql
  libqt4-sql-mysql libqt4-xml libqt4-xmlpatterns libqtcore4 libqtdbus4 libqtgui4 qdbus qt-at-spi
  qtchooser qtcore4-l10n scap-workbench ssh-askpass
0 upgraded, 19 newly installed, 0 to remove and 358 not upgraded.
Need to get 13,0 MB of archives.
After this operation, 47,5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

ANEXO C

Validaciones de Conectividad e Instalación de Paquetes en Clientes

Detalles del cliente a hardenizar

VM: UbuntuSrv18.04-UBA-TFM-C1

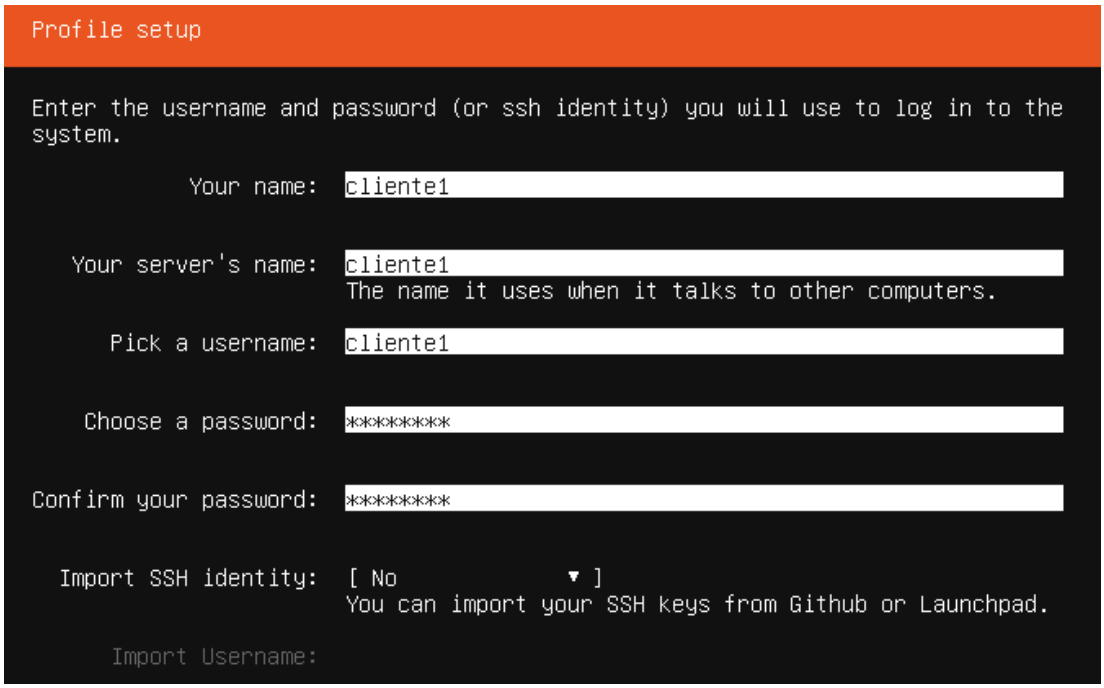
Usuario: cliente1

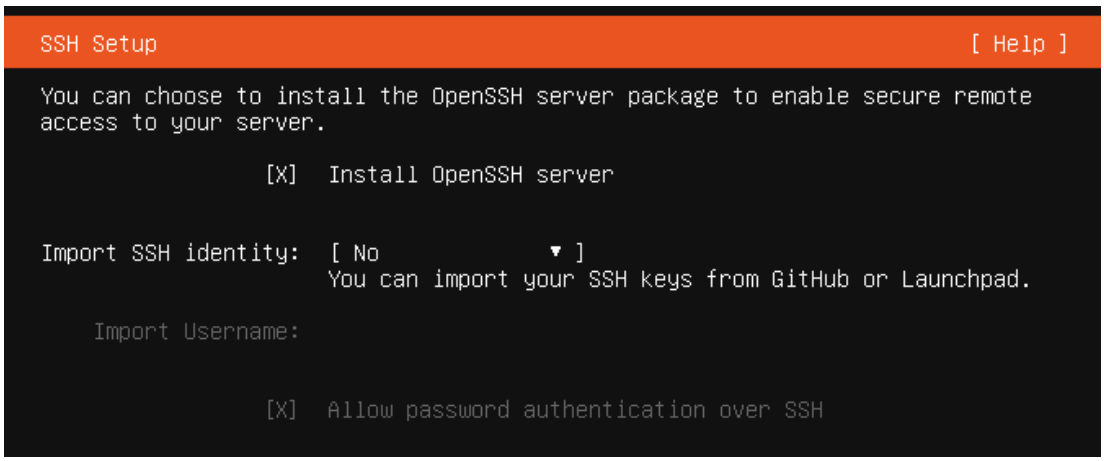
Contraseña: cliente1

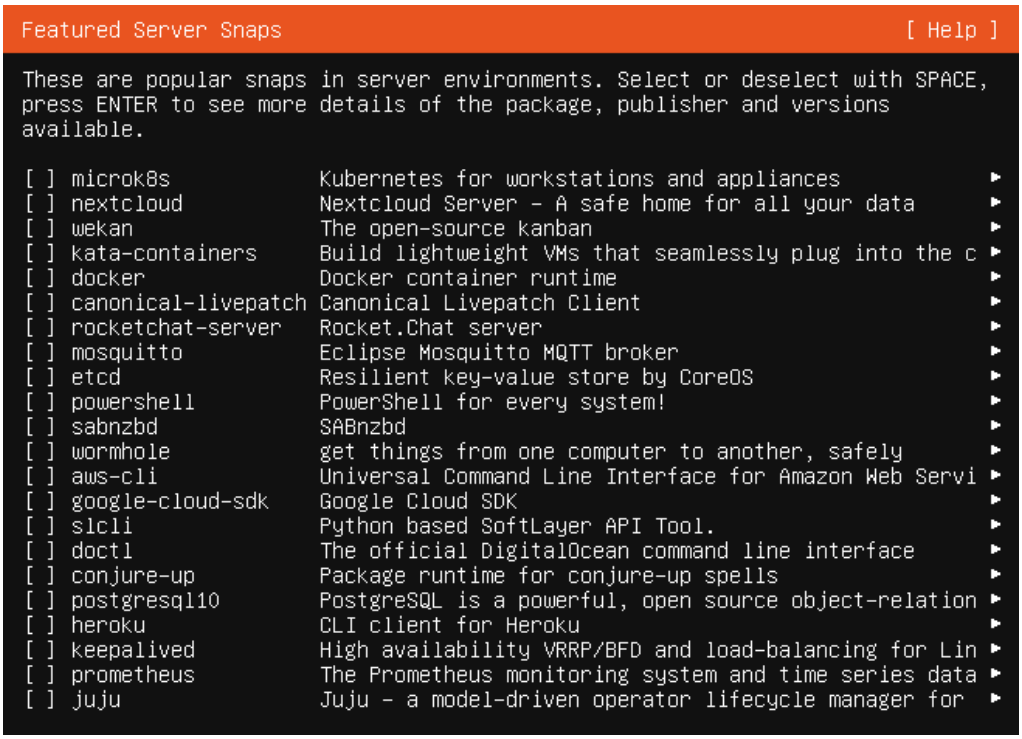
Dirección IP: 10.0.0.21

Sistema Operativo: Ubuntu 18.04

Para las pruebas realizadas, el cliente a hardenizar tendrá instalado únicamente ssh y oscap, los otros paquetes deben estar sin seleccionar durante la instalación del sistema operativo.

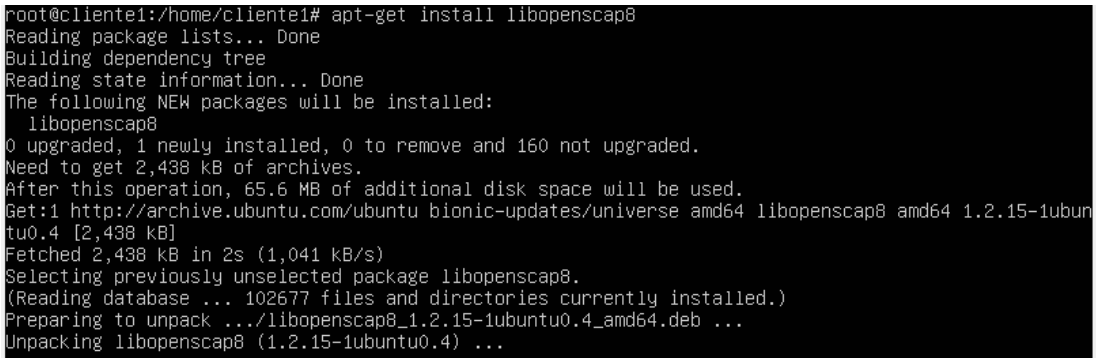






Instalación de oscap en el cliente

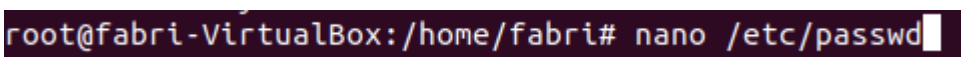
$ apt-get install libopenscap8

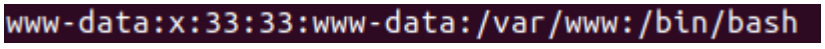


Aceptación del “ssh fingerprint” del cliente desde el usuario www:data en el servidor

Además de agregar al cliente a través de la interfaz web del sistema, se debe aceptar el “ssh fingerprint” de cada cliente agregado, para lo cual se deben seguir los siguientes pasos manuales en el servidor web que publica el Sistema de Hardening Centralizado.

Por primera y única vez, asignar shell a www-data:





Crear la carpeta .ssh y dar permisos a www-data:

```
608  mkdir /var/www/.ssh
609  chown www-data:www-data /var/www/.ssh
```

Adicionalmente, por cada cliente agregado, logearse con el usuario www-data, conectar al cliente vía ssh y aceptar el “fingerprint”:

```
root@fabri-VirtualBox:/home/fabri# su www-data
www-data@fabri-VirtualBox:/home/fabri$ ssh cliente1@10.0.0.21
The authenticity of host '10.0.0.21 (10.0.0.21)' can't be established.
ECDSA key fingerprint is SHA256:XV8x/OpnG46bvFQd1H/MvuQ+vMF4Ivd65vkwFTGTjVg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.21' (ECDSA) to the list of known hosts.
cliente1@10.0.0.21's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Oct 26 03:30:23 UTC 2023

  System load:  0.08              Processes:             103
  Usage of /:   64.9% of 3.86GB   Users logged in:       0
  Memory usage: 19%               IP address for enp0s3: 10.0.0.21
  Swap usage:   0%                IP address for enp0s8: 192.168.1.209


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

132 packages can be updated.
1 update is a security update.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Oct 24 03:13:47 2023
cliente1@cliente1:~$ exit
logout
```

ANEXO D

Detalle de las Pruebas de Validación de Hipótesis

Cliente Objetivo

Se muestra a continuación la versión y dirección IP del cliente objetivo.

```
cliente1@cliente1:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.1 LTS
Release:        18.04
Codename:       bionic
cliente1@cliente1:~$ ip a sh enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:45:03:43 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.21/24 brd 10.0.0.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe45:343/64 scope link
       valid_lft forever preferred_lft forever
cliente1@cliente1:~$
```

Escaneo con Profile for ANSSI DAT-NT28 Average (Intermediate) Level

Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average

Antes de la aplicación de hardening.

Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.EbHSIpdio2/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_averag
Started at	2023-10-29T23:26:00
Finished at	2023-10-29T23:26:01
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4	127.0.0.1
IPv4	10.0.0.21
IPv4	192.168.1.203
IPv6	0:0:0:0:0:0:0:1
IPv6	fe80:0:0:0:a00:27ff:fe45:343
IPv6	fe80:0:0:0:a00:27ff:fe11:70bc
MAC	00:00:00:00:00:00
MAC	08:00:27:45:03:43
MAC	08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 15 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

21 passed | 15 failed | 4 other

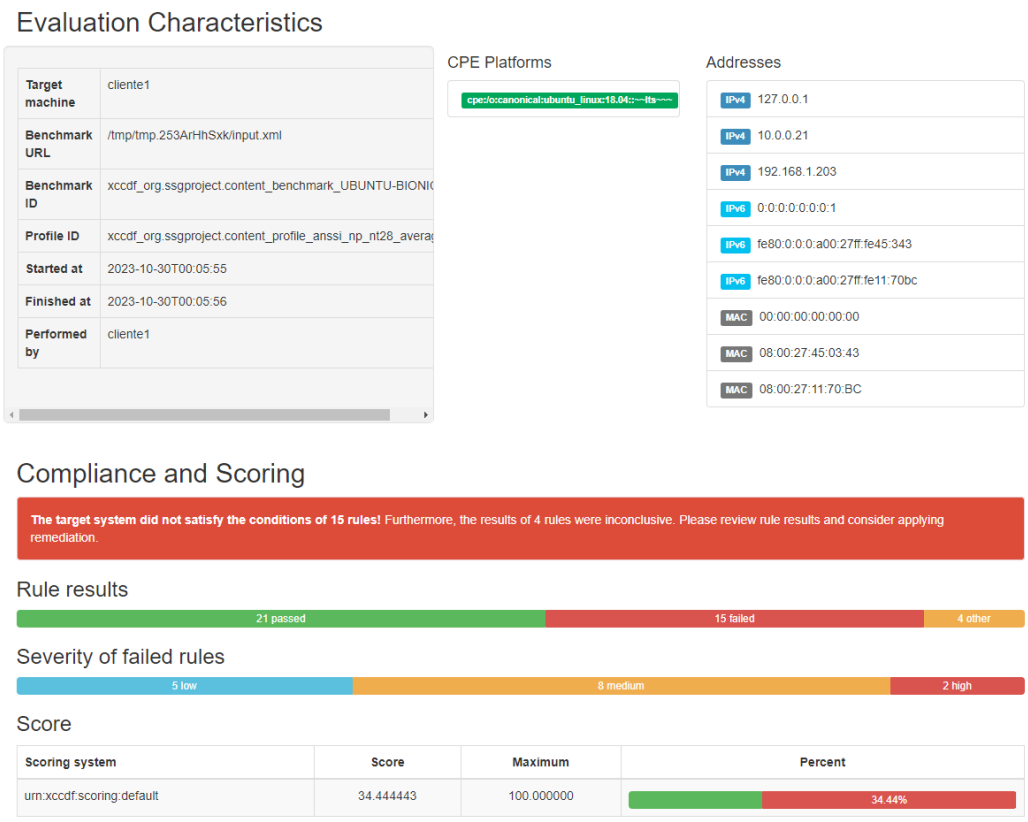
Severity of failed rules

5 low | 8 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	34.444443	100.000000	34.44%

Después de la aplicación de hardening.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.253ArHhSxk/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONI(
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_avera
Started at	2023-10-30T00:05:55
Finished at	2023-10-30T00:05:56
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 15 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

21 passed | 15 failed | 4 other

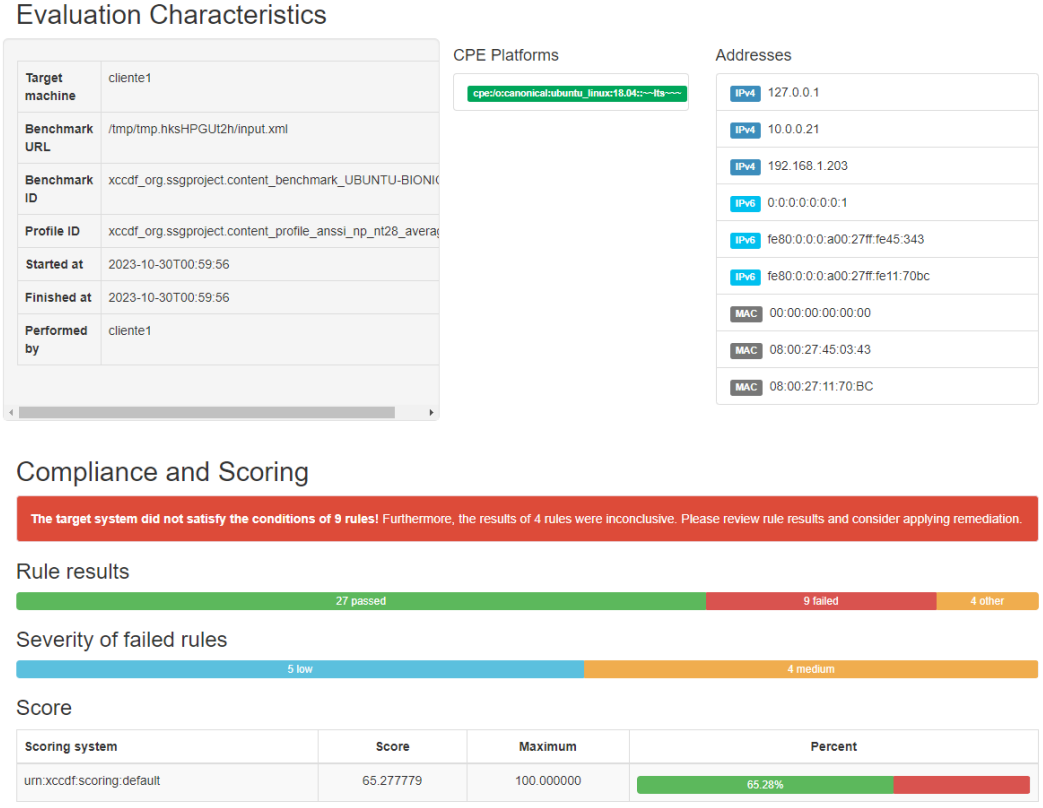
Severity of failed rules

5 low | 8 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	34.444443	100.000000	34.44%

Tras la aplicación de hardening con script modificado.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.hksHPGUt2h/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONI(
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_avera
Started at	2023-10-30T00:59:56
Finished at	2023-10-30T00:59:56
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 9 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

27 passed | 9 failed | 4 other

Severity of failed rules

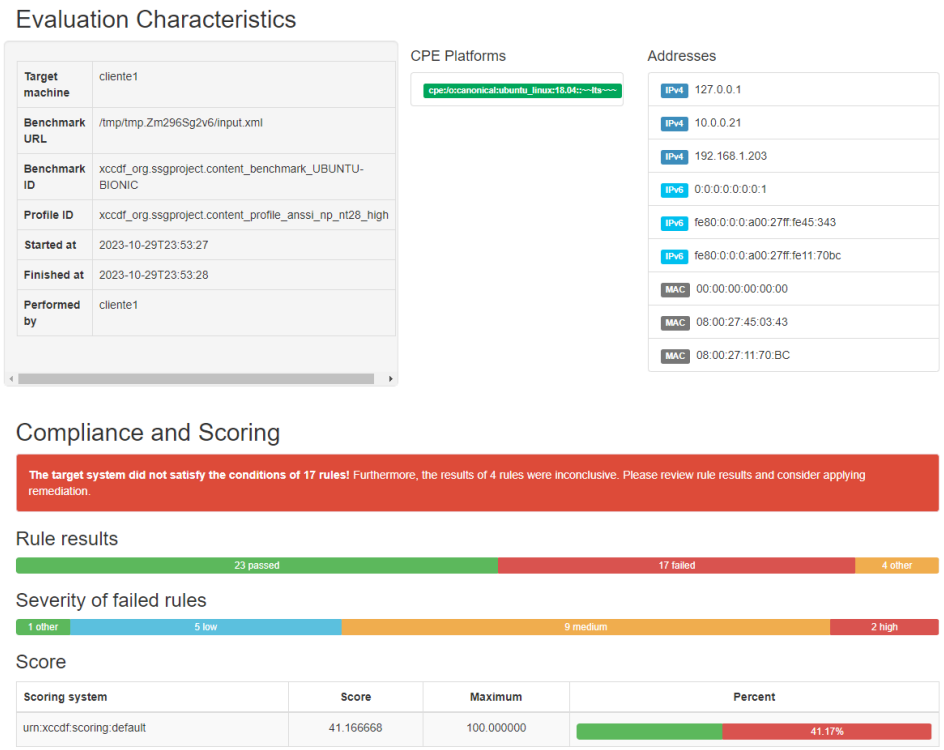
5 low | 4 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	65.277779	100.000000	65.28%

Escaneo con Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)

Antes de la aplicación de hardening.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.Zm296Sg2v6/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_high
Started at	2023-10-29T23:53:27
Finished at	2023-10-29T23:53:28
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 17 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

23 passed | 17 failed | 4 other

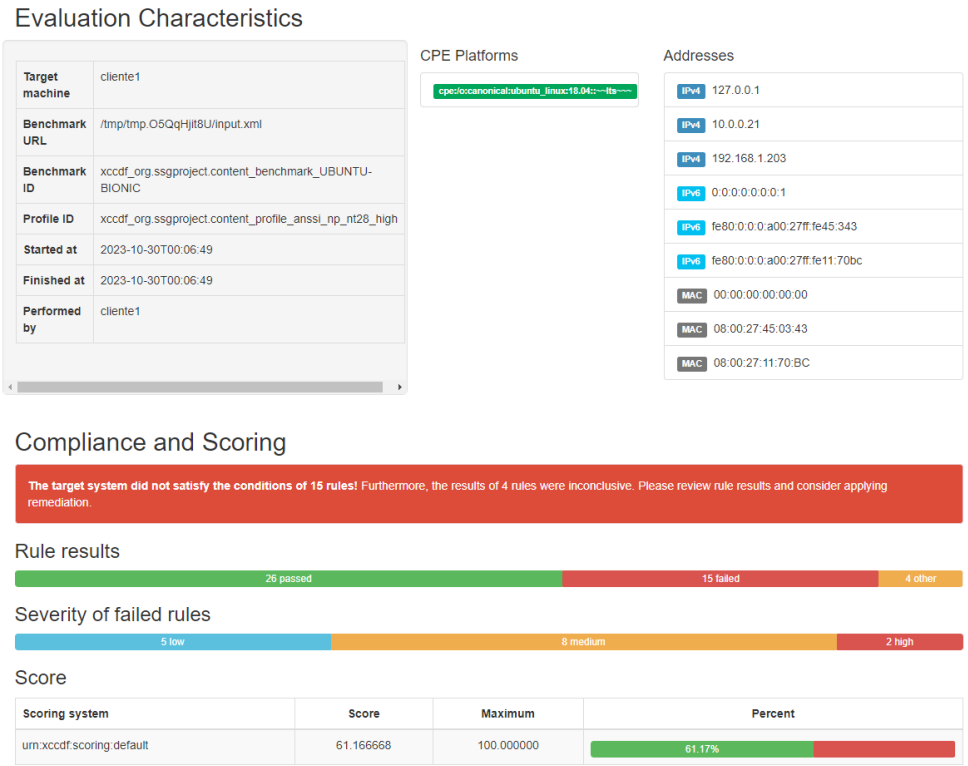
Severity of failed rules

1 other | 5 low | 9 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	41.166668	100.000000	41.17%

Después de la aplicación de hardening.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.O5QqHjlt8U/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_org.ssgproject.content_profile_anssi_np_nt28_high
Started at	2023-10-30T00:06:49
Finished at	2023-10-30T00:06:49
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 15 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

26 passed | 15 failed | 4 other

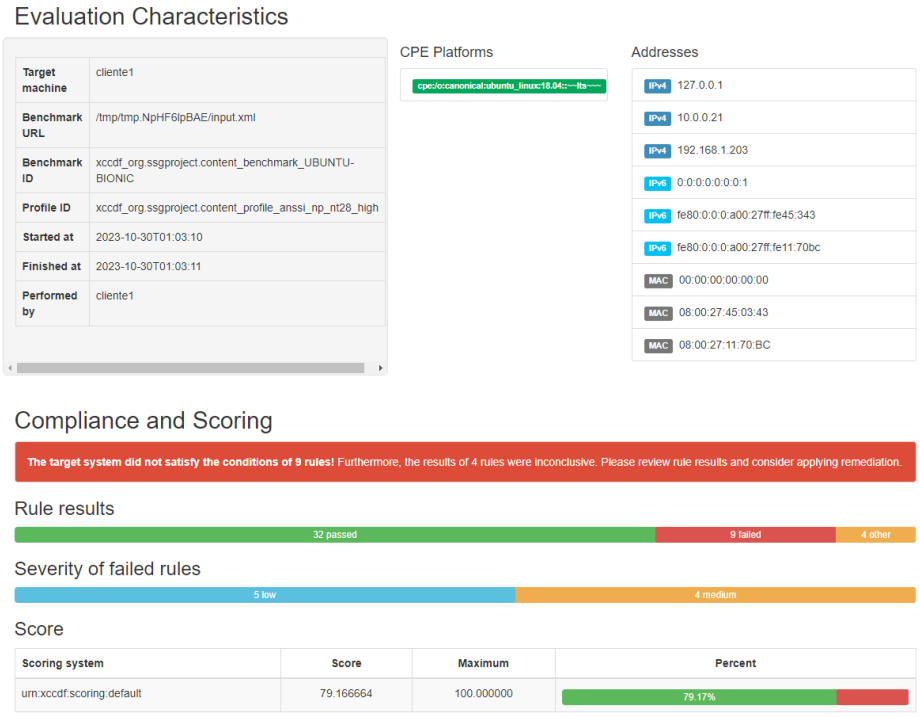
Severity of failed rules

5 low | 8 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	61.166668	100.000000	61.17%

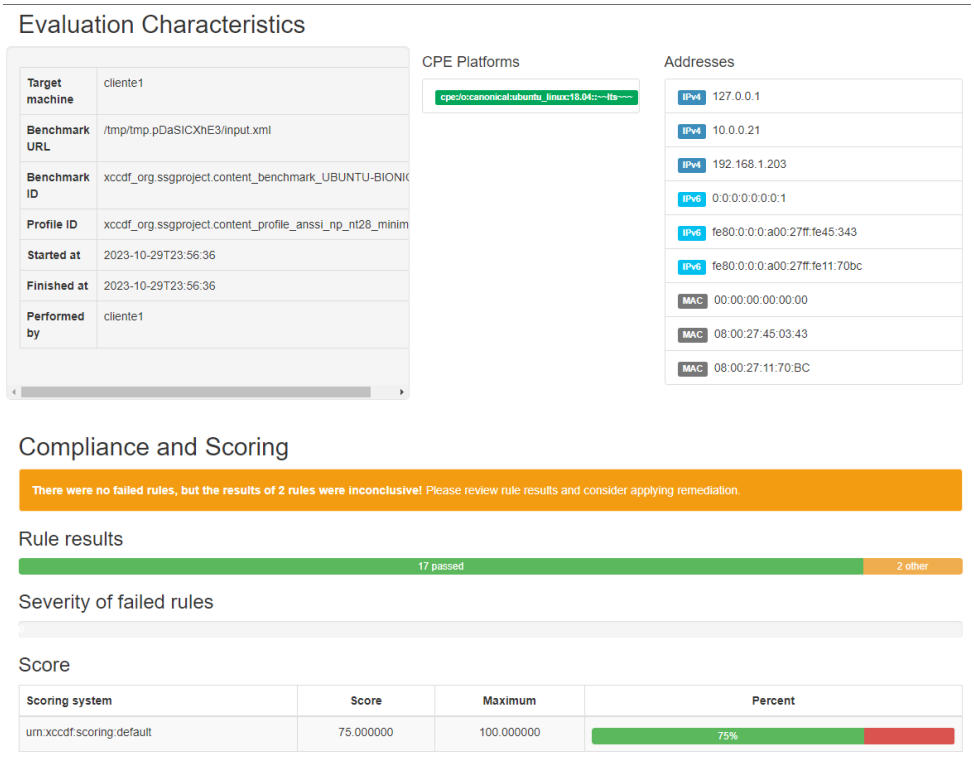
Tras la aplicación de hardening con script modificado.



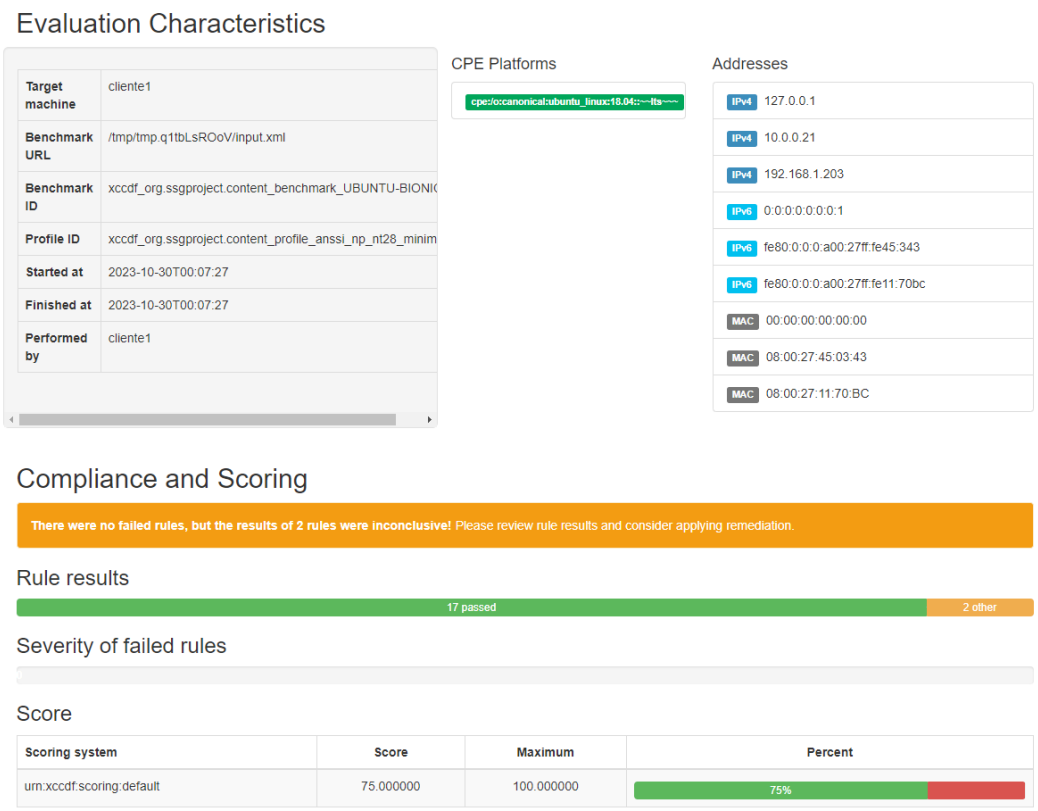
Escaneo con Profile for ANSSI DAT-NT28 Minimal Level

(Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)

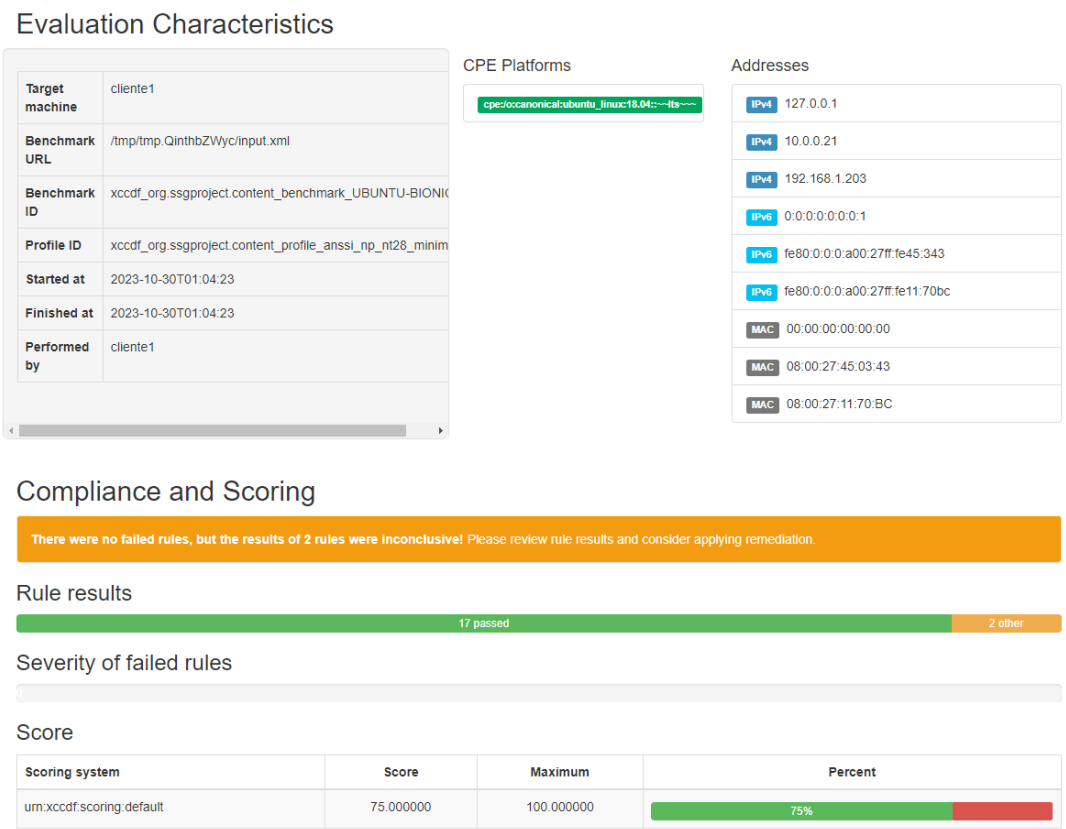
Antes de la aplicación de hardening.



Después de la aplicación de hardening.



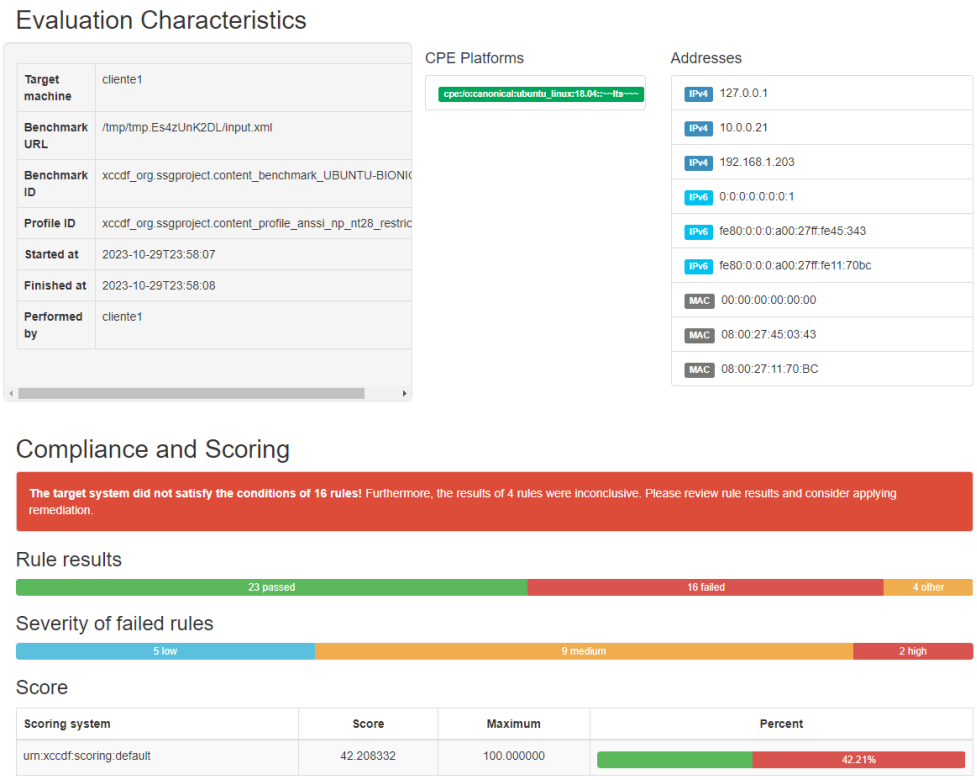
Tras la aplicación de hardening con script modificado.



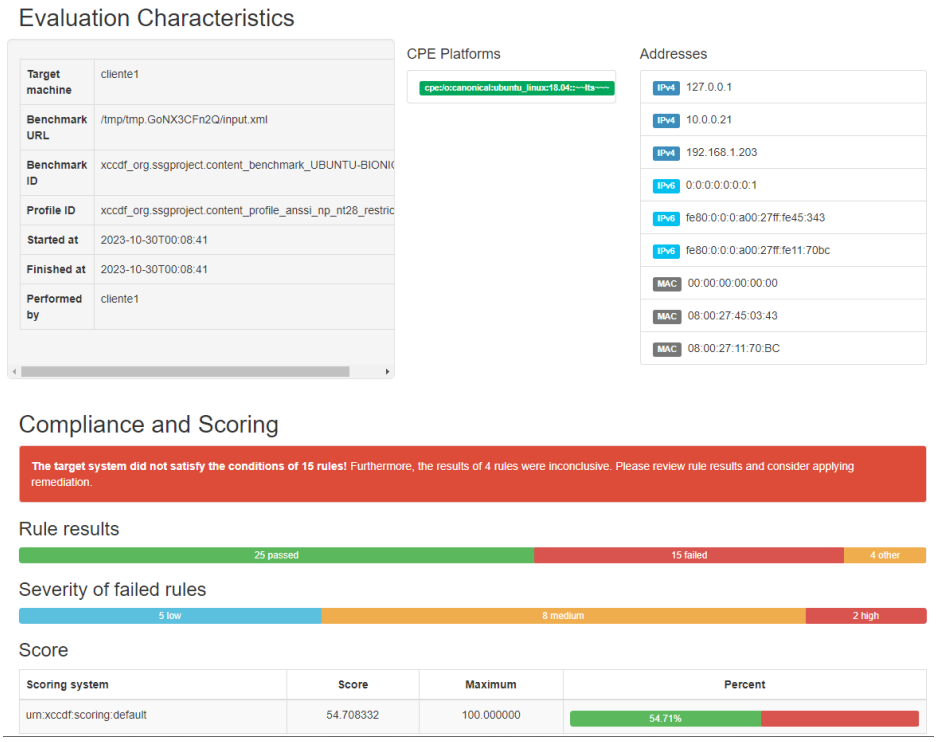
Escaneo con Profile for ANSSI DAT-NT28 Restrictive Level

(Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)

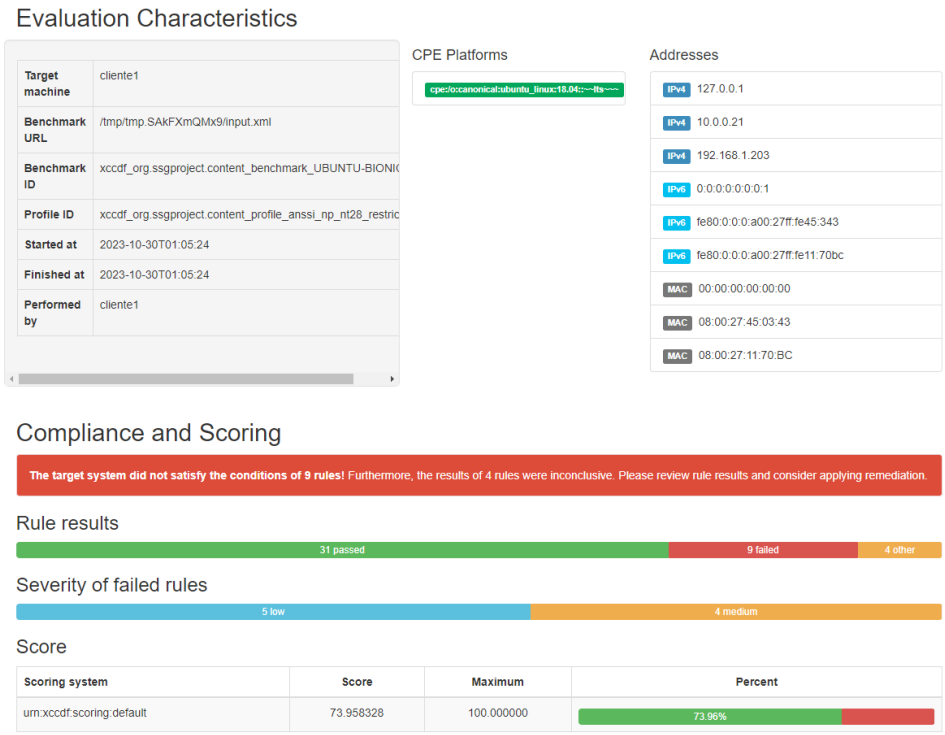
Antes de la aplicación de hardening.



Después de la aplicación de hardening.



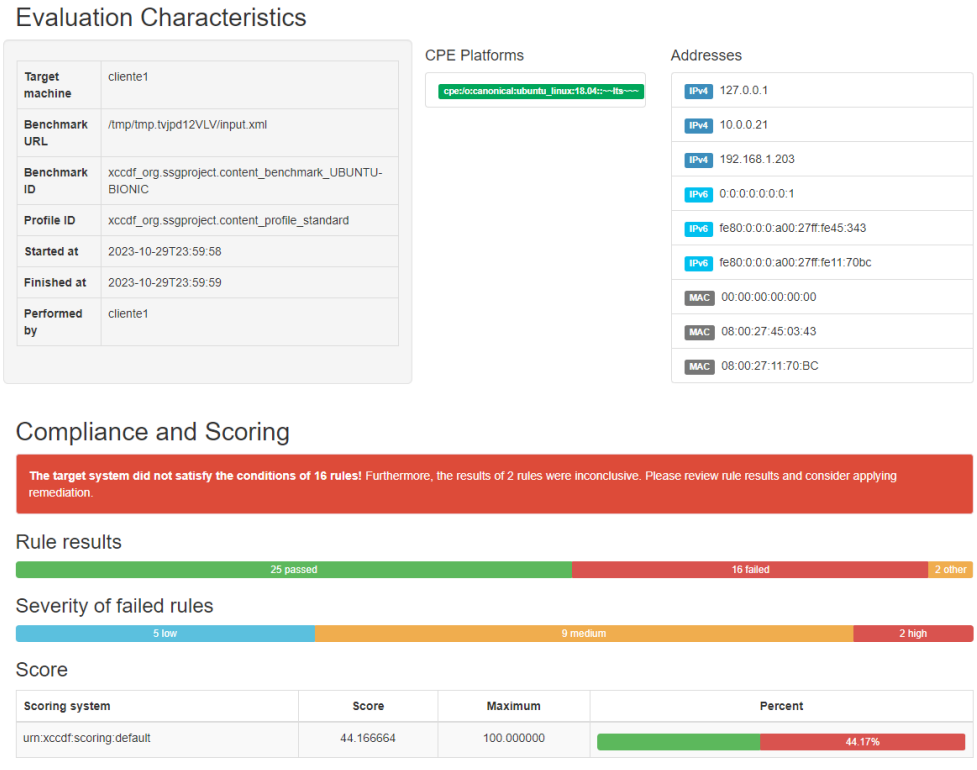
Tras la aplicación de hardening con script modificado.



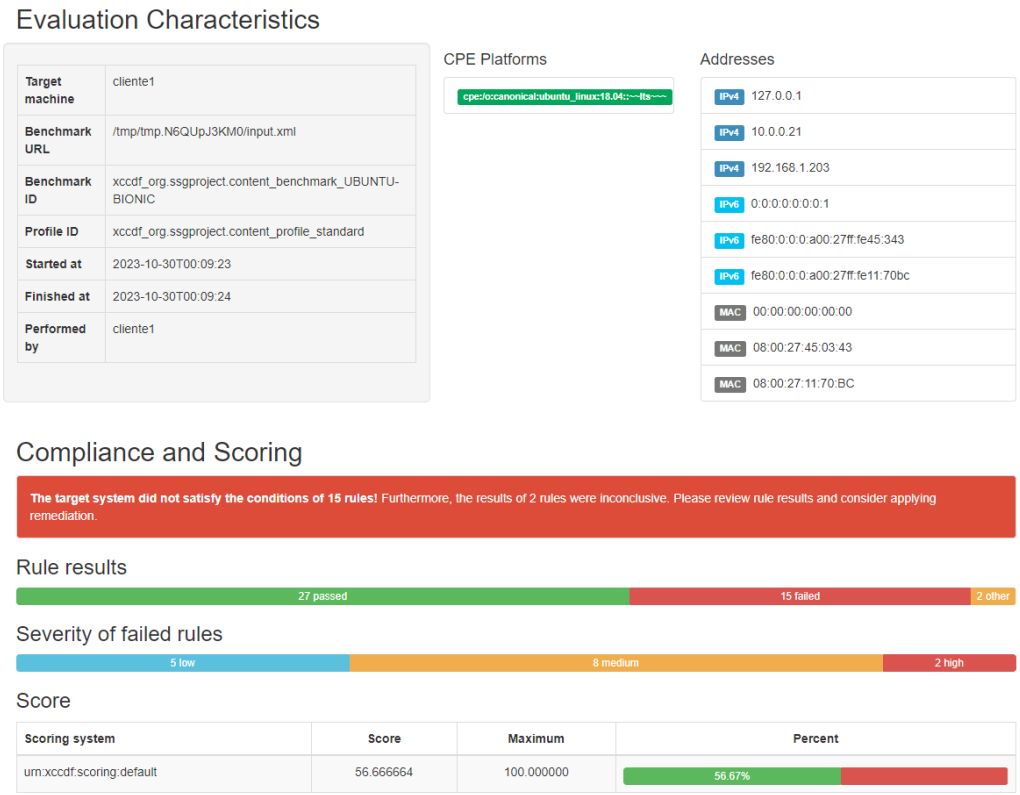
Escaneo con Standard System Security Profile for Ubuntu 18.04

(Id: xccdf_org.ssgproject.content_profile_standard)

Antes de la aplicación de hardening.



Después de la aplicación de hardening.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.N6QUpJ3KM0/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2023-10-30T00:09:23
Finished at	2023-10-30T00:09:24
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 15 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

27 passed | 15 failed | 2 other

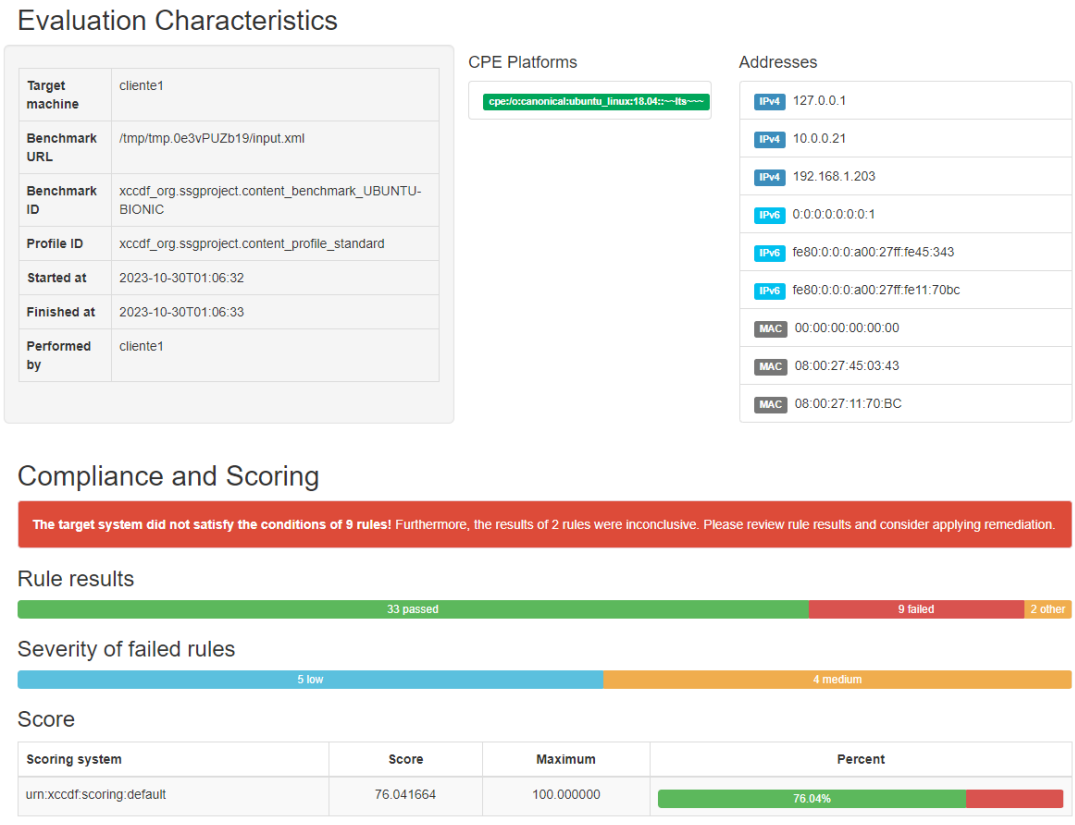
Severity of failed rules

5 low | 8 medium | 2 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	56.666664	100.000000	56.67%

Tras la aplicación de hardening con script modificado.



Evaluation Characteristics

Target machine	cliente1
Benchmark URL	/tmp/tmp.0e3vPUZb19/input.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU-BIONIC
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2023-10-30T01:06:32
Finished at	2023-10-30T01:06:33
Performed by	cliente1

CPE Platforms

cpe:/o:canonical:ubuntu_linux:18.04::~~lts~~~

Addresses

IPv4 127.0.0.1
IPv4 10.0.0.21
IPv4 192.168.1.203
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a00:27ff:fe45:343
IPv6 fe80:0:0:0:a00:27ff:fe11:70bc
MAC 00:00:00:00:00:00
MAC 08:00:27:45:03:43
MAC 08:00:27:11:70:BC

Compliance and Scoring

The target system did not satisfy the conditions of 9 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

33 passed | 9 failed | 2 other

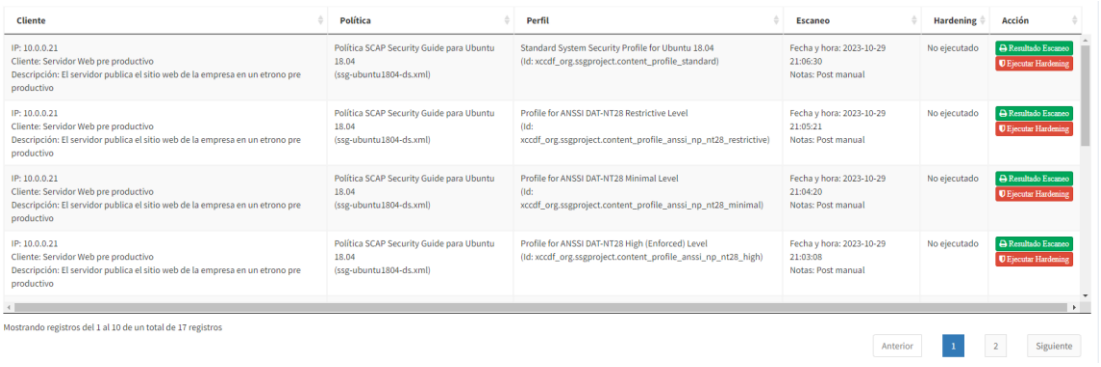
Severity of failed rules

5 low | 4 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	76.041664	100.000000	76.04%

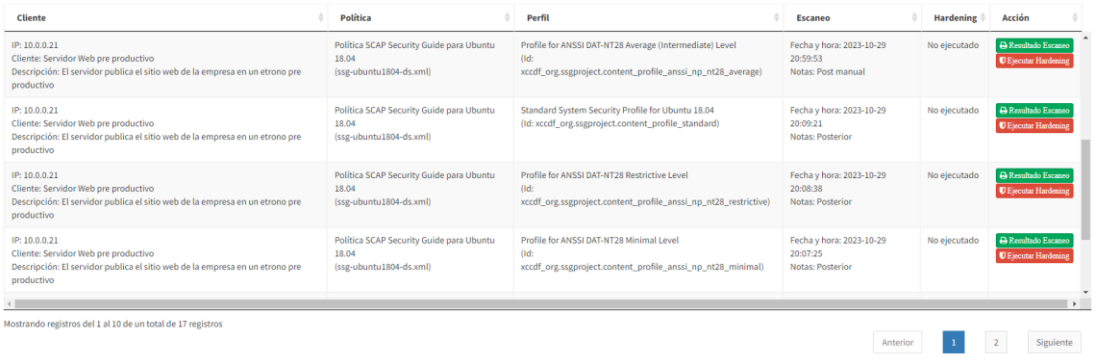
Evidencia de la ejecución de hardening



Cliente	Política	Perfil	Escaneo	Hardening	Acción
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Standard System Security Profile for Ubuntu 18.04 (Id: xccdf_org.ssgproject.content_profile_standard)	Fecha y hora: 2023-10-29 21:06:30 Notas: Post manual	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	Fecha y hora: 2023-10-29 21:05:21 Notas: Post manual	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Minimal Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)	Fecha y hora: 2023-10-29 21:04:20 Notas: Post manual	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)	Fecha y hora: 2023-10-29 21:03:08 Notas: Post manual	No ejecutado	Resultado Escaneo Ejecutar Hardening

Mostrando registros del 1 al 10 de un total de 17 registros

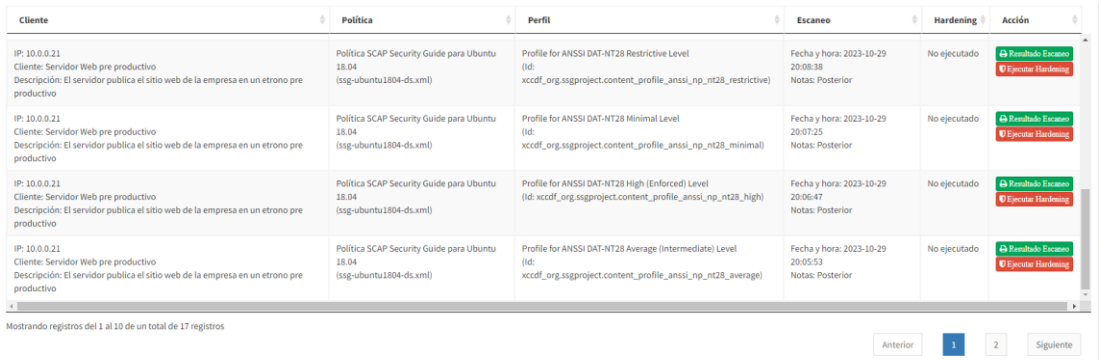
Anterior 1 2 Siguiente



Cliente	Política	Perfil	Escaneo	Hardening	Acción
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Average (Intermediate) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average)	Fecha y hora: 2023-10-29 20:59:53 Notas: Post manual	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Standard System Security Profile for Ubuntu 18.04 (Id: xccdf_org.ssgproject.content_profile_standard)	Fecha y hora: 2023-10-29 20:09:21 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	Fecha y hora: 2023-10-29 20:08:38 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Minimal Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)	Fecha y hora: 2023-10-29 20:07:25 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening

Mostrando registros del 1 al 10 de un total de 17 registros

Anterior 1 2 Siguiente



Cliente	Política	Perfil	Escaneo	Hardening	Acción
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	Fecha y hora: 2023-10-29 20:08:38 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Minimal Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_minimal)	Fecha y hora: 2023-10-29 20:07:25 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)	Fecha y hora: 2023-10-29 20:06:47 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Average (Intermediate) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average)	Fecha y hora: 2023-10-29 20:05:53 Notas: Posterior	No ejecutado	Resultado Escaneo Ejecutar Hardening

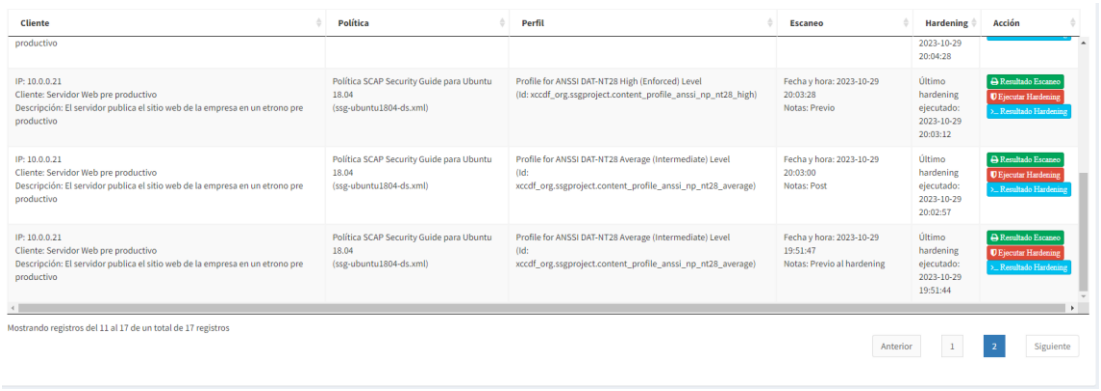
Mostrando registros del 1 al 10 de un total de 17 registros

Anterior 1 2 Siguiente

Cliente	Política	Perfil	Escaneo	Hardening	Acción
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Standard System Security Profile for Ubuntu 18.04 (Id: xccdf_org.ssgproject.content_profile_standard)	Fecha y hora: 2023-10-29 20:05:07 Notas: Previo	Último hardening ejecutado: 2023-10-29 20:05:03	Resultado Escaneo Ejecutar Hardening Resultado Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	CIS Ubuntu 18.04 LTS Benchmark (Id: xccdf_org.ssgproject.content_profile_cis)	Fecha y hora: 2023-10-29 20:04:53 Notas: Previo	Último hardening ejecutado: 2023-10-29 20:04:50	Resultado Escaneo Ejecutar Hardening Resultado Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Restrictive Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_restrictive)	Fecha y hora: 2023-10-29 20:04:43 Notas: Previo	Último hardening ejecutado: 2023-10-29 20:04:40	Resultado Escaneo Ejecutar Hardening Resultado Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Minimal Level (Id:	Fecha y hora: 2023-10-29 20:04:31 Notas: Previo	Último hardening	Resultado Escaneo Ejecutar Hardening

Mostrando registros del 11 al 17 de un total de 17 registros

Anterior 1 2 Siguiente



Cliente	Política	Perfil	Escaneo	Hardening	Acción
productivo				2023-10-29 20:04:28	
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 High (Enforced) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_high)	Fecha y hora: 2023-10-29 20:03:28 Notas: Previo	Último hardening ejecutado: 2023-10-29 20:03:12	Resultado Escaneo Ejecutar Hardening Resultado Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Average (Intermediate) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average)	Fecha y hora: 2023-10-29 20:03:00 Notas: Post	Último hardening ejecutado: 2023-10-29 20:02:57	Resultado Escaneo Ejecutar Hardening Resultado Hardening
IP: 10.0.0.21 Cliente: Servidor Web pre productivo Descripción: El servidor publica el sitio web de la empresa en un etrono pre productivo	Política SCAP Security Guide para Ubuntu 18.04 (ssg-ubuntu1804-ds.xml)	Profile for ANSSI DAT-NT28 Average (Intermediate) Level (Id: xccdf_org.ssgproject.content_profile_anssi_np_nt28_average)	Fecha y hora: 2023-10-29 19:51:47 Notas: Previo al hardening	Último hardening ejecutado: 2023-10-29 19:51:44	Resultado Escaneo Ejecutar Hardening Resultado Hardening

Mostrando registros del 11 al 17 de un total de 17 registros

Anterior 1 2 Siguiente

```
> sh 2023-10-29_20-02-57_id_escaneo_2.sh

[sudo] password for cliente1: Remediating rule 1/15: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/15: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/15: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 6/15: 'xccdf_org.ssgproject.content_rule_rsyslog_files_groupownership'
/home/cliente1/2023-10-29_20-02-57_id_escaneo_2.sh: 64: /home/cliente1/2023-10-29_20-02-57_id_escaneo_2.sh: Syntax error: redirection
unexpected
```

Descargar Script de Hardenización

```
> sh 2023-10-29_20-03-12_id_escaneo_3.sh

[sudo] password for cliente1: Remediating rule 1/17: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/17: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/17: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/17: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/17: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 6/17: 'xccdf_org.ssgproject.content_rule_package_audit_installed'
Reading package lists...
Building dependency tree...
Reading state information...
The following additional packages will be installed:
libauparse0
Suggested packages:
audispd-plugins
The following NEW packages will be installed:
auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 160 not upgraded.
Need to get 243 kB of archives.
After this operation, 803 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libauparse0 amd64 1:2.8.2-1ubuntu1.1 [48.8 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 auditd amd64 1:2.8.2-1ubuntu1.1 [194 kB]
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
LANGUAGE = (unset),
LC_ALL = (unset),
LC_TIME = "es_BO.UTF-8",
LC_MONETARY = "es_BO.UTF-8",
LC_ADDRESS = "es_BO.UTF-8",
LC_TELEPHONE = "es_BO.UTF-8",
LC_NAME = "es_BO.UTF-8",
LC_MEASUREMENT = "es_BO.UTF-8",
LC_IDENTIFICATION = "es_BO.UTF-8",
LC_NUMERIC = "es_BO.UTF-8",
LC_PAPER = "es_BO.UTF-8",
LANG = "en_US.UTF-8"
are supported and installed on your system.
perl: warning: Falling back to a fallback locale ("en_US.UTF-8").
locale: Cannot set LC_ALL to default locale: No such file or directory
Fetched 243 kB in 2s (152 kB/s)
```

```
Selecting previously unselected package libauparse0:amd64.
(Reading database ...
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 103359 files and directories currently installed.)
Preparing to unpack .../libauparse0_1%3a2.8.2-1ubuntu1.1_amd64.deb ...
Unpacking libauparse0:amd64 (1:2.8.2-1ubuntu1.1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a2.8.2-1ubuntu1.1_amd64.deb ...
Unpacking auditd (1:2.8.2-1ubuntu1.1) ...
Setting up libauparse0:amd64 (1:2.8.2-1ubuntu1.1) ...
Setting up auditd (1:2.8.2-1ubuntu1.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service ? /lib/systemd/system/auditd.service.
Processing triggers for systemd (237-3ubuntu10.57) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Remediating rule 7/17: 'xccdf_org.ssgproject.content_rule_grub2_enable_iommu_force'
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/50-curtin-settings.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-4.15.0-213-generic
Found initrd image: /boot/initrd.img-4.15.0-213-generic
Found linux image: /boot/vmlinuz-4.15.0-29-generic
Found initrd image: /boot/initrd.img-4.15.0-29-generic
done
```

```
Remediating rule 8/17: 'xccdf_org.ssgproject.content_rule_rsyslog_files_groupownership'
/home/cliente1/2023-10-29_20-03-12_id_escaneo_3.sh: 104: /home/cliente1/2023-10-29_20-03-12_id_escaneo_3.sh: Syntax error: redirection
unexpected
```

Descargar Script de Hardenización

Evidencia de la ejecución de scripts modificados

```
root@cliente1:/home/cliente1# sh 2023-10-29_19-51-44_id_escaneo_1_modificado.sh
Remediating rule 1/15: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/15: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/15: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 8/15: 'xccdf_org.ssgproject.content_rule_ensure_logrotate_activated'
Remediating rule 11/15: 'xccdf_org.ssgproject.content_rule_package_ntp_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
ntp is already the newest version (1:4.2.8p10+dfsg-5ubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 12/15: 'xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0'
Remediating rule 13/15: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 14/15: 'xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 15/15: 'xccdf_org.ssgproject.content_rule_sshd_disable_root_login'
root@cliente1:/home/cliente1#
```

```
root@cliente1:/home/cliente1# sh 2023-10-29_20-02-57_id_escaneo_2_modificado.sh
Remediating rule 1/15: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/15: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/15: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/15: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 8/15: 'xccdf_org.ssgproject.content_rule_ensure_logrotate_activated'
Remediating rule 11/15: 'xccdf_org.ssgproject.content_rule_package_ntp_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
ntp is already the newest version (1:4.2.8p10+dfsg-5ubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 12/15: 'xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0'
Remediating rule 13/15: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 14/15: 'xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 15/15: 'xccdf_org.ssgproject.content_rule_sshd_disable_root_login'
root@cliente1:/home/cliente1# _
```

```
root@cliente1:/home/cliente1# sh 2023-10-29_20-03-12_id_escaneo_3_modificado.sh
Remediating rule 1/17: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/17: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/17: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/17: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/17: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 6/17: 'xccdf_org.ssgproject.content_rule_package_audit_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
auditd is already the newest version (1:2.8.2-1ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 7/17: 'xccdf_org.ssgproject.content_rule_grub2_enable_iommu_force'
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/50-curtin-settings.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-4.15.0-213-generic
Found initrd image: /boot/initrd.img-4.15.0-213-generic
Found linux image: /boot/vmlinuz-4.15.0-29-generic
Found initrd image: /boot/initrd.img-4.15.0-29-generic
done
Remediating rule 10/17: 'xccdf_org.ssgproject.content_rule_ensure_logrotate_activated'
Remediating rule 13/17: 'xccdf_org.ssgproject.content_rule_package_ntp_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
ntp is already the newest version (1:4.2.8p10+dfsg-5ubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 14/17: 'xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0'
Remediating rule 15/17: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 16/17: 'xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 17/17: 'xccdf_org.ssgproject.content_rule_sshd_disable_root_login'
root@cliente1:/home/cliente1# _
```

```
root@cliente1:/home/cliente1# sh 2023-10-29_20-04-40_id_escaneo_5_modificado.sh
Remediating rule 1/16: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/16: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/16: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/16: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/16: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 6/16: 'xccdf_org.ssgproject.content_rule_package_audit_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
auditd is already the newest version (1:2.8.2-1ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 9/16: 'xccdf_org.ssgproject.content_rule_ensure_logrotate_activated'
Remediating rule 12/16: 'xccdf_org.ssgproject.content_rule_package_ntp_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
ntp is already the newest version (1:4.2.8p10+dfsg-5ubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 13/16: 'xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0'
Remediating rule 14/16: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 15/16: 'xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 16/16: 'xccdf_org.ssgproject.content_rule_sshd_disable_root_login'
root@cliente1:/home/cliente1# _
```

```
root@cliente1:/home/cliente1# sh 2023-10-29_20-05-03_id_escaneo_7_modificado.sh
Remediating rule 1/16: 'xccdf_org.ssgproject.content_rule_partition_for_home'
Remediating rule 2/16: 'xccdf_org.ssgproject.content_rule_partition_for_tmp'
Remediating rule 3/16: 'xccdf_org.ssgproject.content_rule_partition_for_var'
Remediating rule 4/16: 'xccdf_org.ssgproject.content_rule_partition_for_var_log'
Remediating rule 5/16: 'xccdf_org.ssgproject.content_rule_partition_for_var_log_audit'
Remediating rule 6/16: 'xccdf_org.ssgproject.content_rule_package_audit_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
auditd is already the newest version (1:2.8.2-1ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 9/16: 'xccdf_org.ssgproject.content_rule_ensure_logrotate_activated'
Remediating rule 12/16: 'xccdf_org.ssgproject.content_rule_package_ntp_installed'
Reading package lists... Done
Building dependency tree
Reading state information... Done
ntp is already the newest version (1:4.2.8p10+dfsg-5ubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
Remediating rule 13/16: 'xccdf_org.ssgproject.content_rule_sshd_set_keepalive_0'
Remediating rule 14/16: 'xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout'
Remediating rule 15/16: 'xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords'
Remediating rule 16/16: 'xccdf_org.ssgproject.content_rule_sshd_disable_root_login'
root@cliente1:/home/cliente1#
```

BIBLIOGRAFÍA

[1] SEAS, «Hardening: qué es y cómo endurecer las medidas de seguridad informáticas,» SEAS, Estudios superiores abiertos, 9 03 2021. [En línea]. Available: https://www.seas.es/blog/informatica/hardening-que-es-y-como-endurecer-las-medidas-de-seguridad-informaticas/. [Último acceso: 16 06 2022].

[2] «Endurecimiento (informática),» Wikipedia, 12 7 2020. [En línea]. Available: https://es.wikipedia.org/wiki/Endurecimiento_(inform%C3%A1tica). [Último acceso: 16 6 2022].

[3] G. S. -. P. Castro, «Tips tecnológicos, de configuración y negocio que complementan tu seguridad,» 03 05 2012. [En línea]. Available: https://blog.smartekh.com/que-es-hardening. [Último acceso: 16 6 2022].

[4] CISET, Centro de Innovación y Soluciones Empresariales y Tecnológicas, «Hardening,» CISET, Centro de Innovación y Soluciones Empresariales y Tecnológicas, 17 05 2022. [En línea]. Available: https://www.ciset.es/publicaciones/blog/746-hardening. [Último acceso: 16 6 2022].

[5] Ibis Computer, «Hardening informático, ¿qué es?,» [En línea]. Available: https://www.ibiscomputer.com/blog/122-hardening-informatico-que-es. [Último acceso: 16 6 2022].

[6] D. M. C. Monterroso, «Hardening,» Cyber Secuirty, Inormación & Privacidad, 30 4 2021. [En línea]. Available: https://csecmagazine.com/2021/04/30/hardening/#:~:text=Resumen%3A%20Hardening%20es%20un%20t%C3%A9rmino,pueden%20ser%20provocadas%20por%20una. [Último acceso: 16 6 2022].

[7] A. Lopez, «¿Qué es el HARDENING y sus beneficios? | Curso Ciberseguridad | Alberto López,» Yutube, 27 7 2021. [En línea]. Available: https://www.youtube.com/watch?v=BBMS-WgluOA. [Último acceso: 16 6 2022].

[8] K. Pollack, «Herramientas de Endurecimiento,» CalCom Software, 29 4 2021. [En línea]. Available: https://www.calcomsoftware.com/best-hardening-tools/#configuration. [Último acceso: 16 6 2022].

[9] C. C. f. I. Security, «CIS Center for Internet Security,» [En línea]. Available: https://www.cisecurity.org/. [Último acceso: 16 6 2022].

C. Benchmarks, «CIS Benchmarks,» [En línea]. Available: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq. [Último acceso: 16 6 2022].

[11] «CIS Build Kits,» [En línea]. Available: https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content/build-kits-faq. [Último acceso: 16 6 2022].

[12] «Download Sample CIS Build Kits,» [En línea]. Available: https://learn.cisecurity.org/build-kits. [Último acceso: 16 6 2022].

[13] «CIS Securesuite Build Kit Content,» [En línea]. Available: https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content. [Último acceso: 16 6 2022].

[14] «Beneficios de CIS SecureSuite,» [En línea]. Available: https://www.cisecurity.org/cis-securesuite/benefits. [Último acceso: 16 6 2022].

[15] «Categorías y precios de CIS SecureSuite,» [En línea]. Available: https://www.cisecurity.org/cis-securesuite/pricing-and-categories. [Último acceso: 16 6 2022].

[16] «CIS CAT - Test your Security Configuration,» [En línea]. Available: https://learn.cisecurity.org/cis-cat-lite. [Último acceso: 16 6 2022].

[17] NIST, «NIST ABOUT US,» [En línea]. Available: https://www.nist.gov/about-nist. [Último acceso: 04 09 2023].

[18] OpenAI, «ChatGPT NIST y NIST SP,» [En línea]. Available: https://chat.openai.com/. [Último acceso: 04 09 2023].

[19] N. NCP, «National Checklist Program NCP,» [En línea]. Available: https://ncp.nist.gov/general. [Último acceso: 03 09 2023].

[20] NIST, «NIST Special Publication 800-70 rev4 National Checklist Program for IT Products – Guidelines for Checklist Users and Developers,» NIST Special Publication 800-70 rev4, nº 4, p. 52, 2018.

[21] NIST, «NIST Checklist Repository,» [En línea]. Available: https://ncp.nist.gov/repository. [Último acceso: 03 09 2023].

[22] OpenSCAP, «Componentes SCAP,» [En línea]. Available: https://www.open-scap.org/features/scap-components/. [Último acceso: 16 10 2023].

[23] OVAL, «OVAL CIS Repository,» [En línea]. Available: https://github.com/CISecurity/OVALRepo. [Último acceso: 16 10 2023].

[24] O. Community, «OVAL Community Guidelines,» [En línea]. Available: https://oval-community-guidelines.readthedocs.io/en/latest/getting-started.html. [Último acceso: 16 10 2023].

[25] SCAP, «OCIL Open Checklist Interactive Language,» [En línea]. Available: https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/ocil. [Último acceso: 16 10 2023].

[26] SCE, «Script Check Engine,» [En línea]. Available: https://www.open-scap.org/features/other-standards/sce/. [Último acceso: 16 10 2023].

[27] CPE, «Official CPE Dictionary,» [En línea]. Available: https://nvd.nist.gov/products/cpe. [Último acceso: 16 10 2023].

[28] S. Institute, «SANS Institute,» [En línea]. Available: https://www.sans.org/about/?msc=main-nav. [Último acceso: 06 09 2023].

[29] OpenAI, «ChatGPT SANS Institute,» [En línea]. Available: https://chat.openai.com/c/b714a14b-c844-4c66-b5c2-961b143c69ae. [Último acceso: 06 09 2023].

[30] DoD, «Departamento de Defensa de los Estados Unidos de América,» [En línea]. Available: https://www.defense.gov/. [Último acceso: 24 09 2023].

[31] DISA, «Defense Information Systems Agency,» [En línea]. Available: https://www.disa.mil/About. [Último acceso: 24 09 2023].

[32] DoD, «DoD Cyber Exchange Public,» [En línea]. Available: https://public.cyber.mil/. [Último acceso: 24 09 2023].

[33] DISA, «STIGs and SRGs,» [En línea]. Available: https://public.cyber.mil/stigs/.

[34] J. Droba, «LinkedIn Security Technical Implementation Guides,» 05 08 2021. [En línea]. Available: https://www.linkedin.com/pulse/security-technical-implementation-guides-joel-droba/. [Último acceso: 24 09 2023].

[35] Titania, «DISA STIG compliance explained,» [En línea]. Available: https://www.titania.com/resources/guides/disa-stig-compliance-explained. [Último acceso: 24 09 2023].

[36] DoD, «SRG / STIG Library Compilations,» [En línea]. Available: https://public.cyber.mil/stigs/compilations/. [Último acceso: 24 09 2023].

[37] DoD, «STIG Viewing Tools,» [En línea]. Available: https://public.cyber.mil/stigs/srg-stig-tools/. [Último acceso: 24 09 2023].

[38] OpenAI, «ChatGPT - ¿Qué es OpenSCAP?,» [En línea]. Available: https://chat.openai.com/c/b714a14b-c844-4c66-b5c2-961b143c69ae. [Último acceso: 16 10 2023].

[39] OpenSCAP, «About the OpenSCAP Family,» [En línea]. Available: https://www.open-scap.org/tools/. [Último acceso: 16 10 2023].

[40] OpenSCAP, «OpenSCAP Standards,» [En línea]. Available: https://www.open-scap.org/features/standards/. [Último acceso: 16 10 2023].

[41] OpenSCAP, «OpenSCAP Base,» [En línea]. Available: https://www.open-scap.org/tools/openscap-base/. [Último acceso: 16 10 2023].

[42] OpenSCAP, «OpenSCAP 1.3 User Manual,» [En línea]. Available: https://static.open-scap.org/openscap-1.3/oscap_user_manual.html. [Último acceso: 16 10 2023].

[43] Š. L. M. P. Peter Vrabec, «oscap - Man Page,» [En línea]. Available: https://www.mankier.com/8/oscap. [Último acceso: 17 10 2023].

[44] OpenSCAP, «SCAP Security Guide,» [En línea]. Available: https://www.open-scap.org/security-policies/scap-security-guide/. [Último acceso: 17 10 2023].

[45] OpenSCAP, «Políticas de seguridad disponibles en la Guía de seguridad de SCAP,» [En línea]. Available: https://www.open-scap.org/security-policies/choosing-policy/. [Último acceso: 17 10 2023].

[46] OpenSCAP, «Openscap-utils,» [En línea]. Available: https://www.mankier.com/package/openscap-utils. [Último acceso: 17 10 2023].

[47] OpenSCAP, «Oscap-ssh,» [En línea]. Available: https://www.mankier.com/8/oscap-ssh. [Último acceso: 17 10 2023].

[48] S. Workbench, «SCAP Workbench User Manual,» [En línea]. Available: https://static.open-scap.org/scap-workbench-1.1/. [Último acceso: 15 10 2023].

[49] Ubuntu, «The Ubuntu Security Guide,» [En línea]. Available: https://ubuntu.com/security/certifications/docs/usg. [Último acceso: 30 09 2023].

[50] Ubuntu, «Installation of the Ubuntu Security Guide,» [En línea]. Available: https://ubuntu.com/security/certifications/docs/disa-stig/installation. [Último acceso: 30 09 2023].

[51] Ubuntu, «Comply with CIS or DISA STIG on Ubuntu 20.04 with Ubuntu Security Guide,» [En línea]. Available:

https://ubuntu.com/tutorials/comply-with-cis-or-disa-stig-on-ubuntu#1-overview. [Último acceso: 30 09 2023].

[52] Ubuntu, «Customizing the CIS profile,» [En línea]. Available: https://ubuntu.com/security/certifications/docs/usg/cis/customization. [Último acceso: 30 09 2023].

[53] Ubuntu, «CIS benchmark compliance: Introducing the Ubuntu Security Guide,» [En línea]. Available: https://ubuntu.com/blog/cis-security-compliance-usg. [Último acceso: 30 09 2023].

[54] Ubuntu, «CIS Benchmark on Ubuntu,» [En línea]. Available: https://ubuntu.com/security/cis. [Último acceso: 30 09 2023].

[55] Ubuntu, «DISA-STIG on Ubuntu,» [En línea]. Available: https://ubuntu.com/security/disa-stig. [Último acceso: 30 09 2023].

[56] Ubuntu, «BastilleLinux,» [En línea]. Available: https://help.ubuntu.com/community/BastilleLinux. [Último acceso: 30 09 2023].

[57] C. FY, «Lynis,» [En línea]. Available: https://cisofy.com/lynis/. [Último acceso: 04 10 2023].

[58] C. FY, «Lynis security controls,» [En línea]. Available: https://cisofy.com/lynis/controls/banner/. [Último acceso: 04 10 2023].

[59] C. FY, «GitHub Lynis,» [En línea]. Available: https://github.com/CISOfy/Lynis. [Último acceso: 04 10 2023].

[60] C. FY, «Get Started with Lynis,» [En línea]. Available: https://cisofy.com/documentation/lynis/get-started/. [Último acceso: 04 10 2023].

[61] GitHub, «JShielder,» [En línea]. Available: https://github.com/Jsitech/JShielder. [Último acceso: 05 10 2023].

[62] J. Soto, «Que es Jshielder?,» [En línea]. Available: https://jsitech1.gitbooks.io/jshielder-linux-server-hardening-script/content/jshielder1.html. [Último acceso: 05 10 2023].

[63] G. K. T. Sjögren, «Hardening Ubuntu,» [En línea]. Available: https://github.com/konstruktoid/hardening. [Último acceso: 08 10 2023].

[64] G. GrapheneX, «GrapheneX Automated System Hardening Framework for Linux & Windows,» [En línea]. Available: https://github.com/grapheneX/grapheneX. [Último acceso: 08 10 2023].

[65] CalCom, «CalCom,» [En línea]. Available: https://www.calcomsoftware.com/company/#about-us. [Último acceso: 03 09 2023].

[66] CalCom, «CalCom Hardening Suite (CHS),» [En línea]. Available: https://www.calcomsoftware.com/server-hardening-suite/. [Último acceso: 03 09 2023].

[67] B. S. -. L. B. D. CalCom, Interviewee, Reunión de presentación de la herramienta CalCom CHS. [Entrevista]. 11 10 2023.

[68] Runecast, «Runecast About Us,» [En línea]. Available: https://www.runecast.com/about-us. [Último acceso: 11 10 2023].

[69] OpenAI, «ChatGPT Runecast - ¿Sabes para que sirve la herramienta Runcast Analyzer?,» [En línea]. Available: https://chat.openai.com/c/b714a14b-c844-4c66-b5c2-961b143c69ae. [Último acceso: 11 10 2023].

[70] Runecast, «Guía de usuario de Runecast Analyzer,» [En línea]. Available: https://demo.runecast.com/rca/user-guide/index.html. [Último acceso: 11 10 2023].

[71] Runecast, «Demo en linea,» [En línea]. Available: https://demo.runecast.com/rca/dashboard. [Último acceso: 11 10 2023].

[72] SteelCloud, «Guía de Usuario de ConfigOS Command Center,» [En línea]. Available: https://www.steelcloud.com/wp-content/uploads/CommandCenter_2.8.4_User_Guide_V2022_03142022_Final.pdf. [Último acceso: 14 10 2023].

[73] CalCom, «CalCom Demo,» [En línea]. Available: https://www.calcomsoftware.com/request-demo/. [Último acceso: 03 09 2023].

[74] CalCom, «CalCom Blog,» [En línea]. Available: https://www.calcomsoftware.com/blogs/. [Último acceso: 03 09 2023].

[75] DISA, «Control Correlation Identifier (CCI),» [En línea]. Available: https://public.cyber.mil/stigs/cci/. [Último acceso: 24 09 2023].

BLIOGRAFÍA GENERAL

- C. Alvarez Martín y P. González Pérez, *Hardening de servidores GNU / Linux.* 4ª Edición. España: 0xWORD, 2020.
- D. Maldonado, *Máxima Seguridad en WordPress.* 1ª Edición. España: 0xWORD, 2016.
- E. Rando, P. González, A. Aparicio, R. Martín y Ch. Alonso, *Hacking Web Technologies.* 2ª Edición. España: 0xWORD, 2020.