IDENTIFICACIÓN Y PROPUESTA DE UNA SOLUCIÓN DE MEJORA A LAS VULNERABILIDADES INFORMÁTICAS DE LA RED Y DEL AMBIENTE DE SERVIDORES DE PREPRODUCCIÓN DE LA ENTIDAD KERALTY

PRESENTADO POR:

HAMILTON BOLAÑOS GONZALEZ

JOSE MANUEL CRUZ CUELLAR

JAVIER REYES PEÑALOZA

ASESOR TÉCNICO DE PROYECTO:

JAIRO HERNÁN GARCIA TRIANA

UNIVERSIDAD EL BOSQUE

FACULTAD DE INGENIERÍA ELECTRÓNICA

ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS

BOGOTÁ, COLOMBIA

11 DE DICIEMBRE DE 2018

Autores: Hamilton Bolaños, Javier Reyes, José Cruz

Director: Jairo García

Investigación IV

Línea: Seguridad en redes telemáticas

Fecha: 11 de diciembre de 2018

RESUMEN

Mediante la evaluación de las plataformas de seguridad y servidores de la infraestructura tecnológica, se idéntico que la entidad Keralty no tenía bien definidas las políticas de seguridad en términos generales, a pesar que esta entidad tiene un departamento de seguridad TI con directivos y administradores trabajando en esta área, este personal no tenía un enfoque detallado del estado actual de la infraestructura de red y de sus vulnerabilidades informáticas, por tal motivo, se realizó depuración de las políticas del firewall interno y un análisis de vulnerabilidades de servidores del ambiente de preproducción de la compañía, así mismo, se planteó una propuesta de solución de mejora de acuerdo a las vulnerabilidades encontradas a los servidores y con relación al firewall se realizó una intervención de acuerdo al manual de buenas prácticas entregado por el fabricante.

Este trabajo brinda una visión panorámica del estado actual a nivel de seguridad TI de la compañía en mención, toda vez que se identificaron las vulnerabilidades en la infraestructura de red. Así mismo, se elaboraron recomendaciones que permiten mitigar los riesgos asociados a las amenazas con el propósito de mejorar la seguridad y la calidad del servicio prestado a los proveedores.

PALABRAS CLAVE

Firewall, IPS, servidores, análisis de vulnerabilidades, análisis de riesgos, seguridad de la información.

ABSTRACT

Through the evaluation of the platforms of security and servers of the technological infrastructure, it was identified that the Keralty entity did not have well-defined security policies in general terms, despite the fact that this entity has an IT security department with managers and administrators working in this area, this staff did not have a detailed approach to the current state of the network infrastructure and its computer vulnerabilities, for this reason, debugging the internal firewall policies and a vulnerability analysis of servers of the preproduction environment of the company, likewise, an improvement solution proposal was proposed according to the vulnerabilities found into the servers and in relation to the firewall an intervention was performed according to the manual of good practices delivered by the manufacturer.

This work provides a panoramic view of the current state at the IT security level of the company in question, since the vulnerabilities in the network infrastructure that were identified. Likewise, recommendations were made to mitigate the risks associated with threats in order to improve the security and quality of the service provided to suppliers.

KEYWORDS

Firewall, IPS, servers, vulnerability analysis, risk analysis, information security.

TABLA DE CONTENIDO

Listado de Tablas

Listado de Figuras

1. Título del proyecto

Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad Keralty.

2. Introducción

Con el acceso a Internet a nivel mundial, la organización ha tiene como propósito implementar métodos de protección en sus sistemas informáticos, con el fin de almacenar confidencialmente la información generada diariamente, logrando así abarcar varias medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras que dependen del usuario, tales como la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet. Alcanzando un nivel de seguridad esperado en pro de conservar y preservar servicios idóneos, además identificar y resolver oportunamente los ajustes y refuerzos requeridos en seguridad a través de los servicios propuestos.

En la organización objeto de estudio se logra rescatar su proceso y trayectoria para generar un proceso de impacto con un antes y después de implementar y promover las estrategias adecuadas para fortalecer sus debilidades, es por eso que la Organización Sanitas Internacional con el objetivo de incursionar en nuevos mercados externos evoluciono a Keralty a partir de 1 de marzo de 2018 para ofrecer una propuesta más fresca y dinámica que le permitirá al grupo empresarial llegar con su marca a más países. Esta empresa tuvo su nacimiento en Colombia en 1980 con la compañía de medicina preparada Keralty, estableciendo en el país un novedoso modelo de aseguramiento privado voluntario denominado Medicina Prepagada. Esto supuso el primer paso para la creación de un hospital y de una estructura administrativa que, actualmente, está presente en todo el país. EPS Sanitas surge como respuesta al sistema colombiano de Seguridad Social con el fin de garantizar la atención establecida en el Plan Obligatorio de Salud (Ley 100/1993). Para cumplir con los servicios incluidos en dicho plan, EPS Sanitas ha desarrollado una extensa red de médicos afiliados, tecnología e infraestructura que constituyen un área médica extendida a lo largo de todo el país [1].

Actualmente EPS Sanitas cuenta con más de 2.624.619 de afiliados, una cobertura geográfica en 210 ciudades y el 91% de los usuarios manifestaron estar satisfechos con el servicio.

3. Descripción general del proyecto

3.1. Definición del problema

En la organización Keralty los mayores incidentes en la seguridad informática se presentaban por diferentes factores que incrementaban los riesgos en la pérdida de la información. Estos factores hacían referencia a malas prácticas en las configuraciones del firewall y de servidores, producto de la falta de habilidades técnicas de los administradores y carencias de políticas de seguridad internas de la empresa que habilitaban los incidentes de indisponibilidad en los servicios de red, identificando que por errores de configuraciones realizadas por los administradores, los usuarios tenían acceso no controlado a Internet lo cual causaban pérdidas de información y la infección de equipos de cómputo, los malos hábitos del área de programadores dejaban brechas abiertas que generaban vulnerabilidades de alto impacto.

3.1.1. Manifestación

La mala administración de los firewalls generaba diferentes eventos de ciberseguridad que prendían las alarmas porque se registraban ataques a las plataformas de Internet de la entidad de bajo nivel, sin embargo, los ataques pasivos y activos tanto externos como internos estaban a la orden del día, exponiendo a las plataformas desde una denegación de servicio hasta el robo sensible de la información de Keralty, las aplicaciones expuestas en los servidores reúnen protocolos de seguridad pero no son actualizados constantemente como si lo hacen las diferentes técnicas de ataques.

El sitio portal.Keralty.com es la URL que más ataques de ciberseguridad recibió, pero en ningún momento se reportaron afectaciones considerables para sus clientes y afiliados, este portal es uno de los más importantes porque presta servicios como historial clínico de sus pacientes, pago en línea, plan médico domiciliario, programas de salud, entre otros, que si se hubiera visto afectado por un ataque de denegación de servicios causaría que los servicios nombrados sean inaccesibles para los usuarios legítimos. Además, la mala administración de los firewalls comprometía la información sensible de Keralty, la cual está obligada a proteger de acuerdo a las leyes colombianas, dado que almacena datos personales de sus clientes y afiliados.

Por supuesto, aparte los ataques nombrados, existen muchos más ataques informáticos que constituían amenazas para la empresa como malware (virus, gusanos, troyanos, spyware,

adware), de otro lado, la falta de concienciación de los empleados en temas de seguridad de la información es otro tema que preocupaba al área de seguridad TIC de Keralty, porque los firewalls no contaban con perfiles webfilter y application control que permitían evitar el acceso no autorizado de los empleados a ciertos sitios de Internet que estaban consumiendo el ancho de banda contratado, y desviando la atención en otras tareas que no son propias de sus funciones asignadas. Así mismo, la falta de capacitación de los empleados en seguridad de la información constituía otro riesgo (aparte de la mala configuración de los firewalls), porque estaban expuestos a técnicas como la ingeniería social utilizada por ciberdelincuentes o la incursión de malware a través de los sitios web visitados, sin tener una orientación de cómo reaccionar frente a incidentes cibernéticos.

3.1.2. Contexto

La última inversión que la compañía realizó para proteger sus activos en cuanto a hardware y software fue implementada con un costo muy elevado, pero no se contó con personal idóneo para la administración de los equipos adquiridos y la divulgación de buenas prácticas de configuración o del valor que genera un activo de la información, durante la compra de los equipos no se contó con el soporte necesario y una evaluación acertada de las herramientas adquiridas incluido su soporte y administración. Esto hizo que la inversión usara un 35% de su capacidad en la cual se presentaban varias vulnerabilidades abiertas a cualquier atacante interesado. La compañía cuenta con cerca de 3.000 empleados entre directos y proveedores y los activos directamente implicados con la seguridad de la compañía son las bases de datos de los usuarios la cual está expuesta en Internet:

- avicena.Keralty.com
- capacitacionvirtualosi.com
- Keralty.com
- descubretusalud.com
- fus.Keralty.com
- optisanitas.com
- osisanitas.com
- osisanitas.com.co
- portal.Keralty.com
- www.capacitacionvirtualosi.com

- www.Keralty.com
- zeus.Keralty.com

De acuerdo al análisis y levantamiento de información realizada, se identificó que el firewall utilizado para protección de las bases de datos y aplicación de Keralty es un punto crítico, debido a que si se llegara a perder su disponibilidad se estaría comprometiendo la continuidad del negocio, ya que su activo principal es la información. Actualmente la compañía tiene la siguiente topología de red.

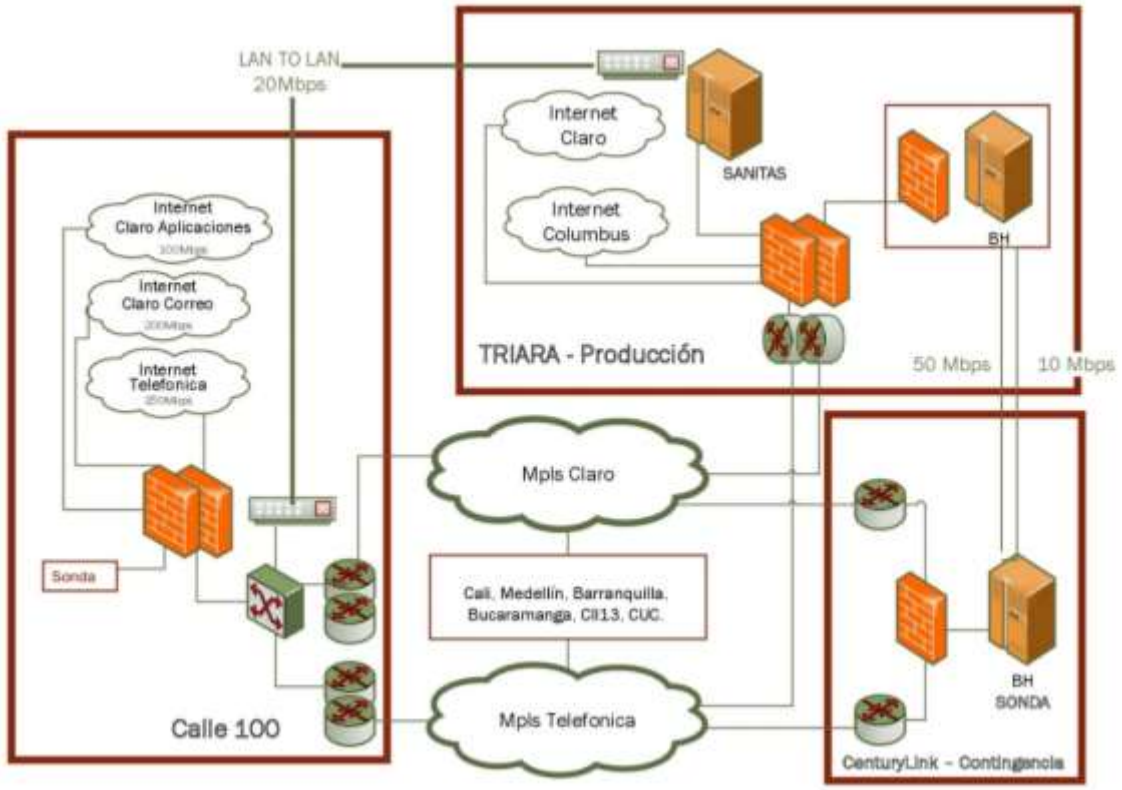


Figura 1: Topología Organización Sanitas

3.1.3. Causas

Se habían identificado constantes ataques de menor impacto que serán detallados más adelante, afortunadamente no se registra en ninguna plataforma el robo de información, pero según los hallazgos si es posible que en algún momento ocurra, como lo vivido en Reino Unido en mayo de 2017, donde según el Sistema Nacional de Salud británico, NHS, confirmo que al menos 25 hospitales y centros médicos por todo el país habían sido víctimas de un ciberataque, pidiendo rescate por ordenador infectado [2].

3.1.4. Efectos

Afortunadamente la compañía no ha sido blanco de un ataque de alto nivel porque de lo contrario su impacto a nivel legal y de credibilidad cambiaría la perspectiva de sus clientes y afiliados quienes indirectamente se verían involucrados.

La amenaza que suponen los virus informáticos a nivel sanitario va mucho más allá del robo y filtración de historiales médicos, aunque esta sea una cuestión de máxima importancia y que merece un análisis propio. Hablamos de cómo afecta un ciberataque a la práctica clínica de un hospital que de repente, tiene que pagar todos sus ordenadores y cortar las comunicaciones telefónicas, cancelar cientos de cirugías programadas, dificultad para acceder a los resultados de pruebas diagnósticas, ni realizar otras como, por ejemplo, radiografías, algo fundamental en la atención de urgencias. Hasta los recién nacidos se verían afectados por un ataque, pues las enfermeras de maternidad no podrían imprimir las etiquetas identificativas.

Es imposible cuantificar en qué medida afectó el ataque a la seguridad de los pacientes colombianos pero, además de comprometer la atención sanitaria habitual de cada uno de los centros afectados (y el efecto cascada en días sucesivos), pudo tener consecuencias importantes en situaciones en las que el tiempo de reacción es fundamental (como en un accidentes de tráfico, un ictus o un infarto). Pero aún más preocupante que el aumento de los ciberataques es que los hospitales no estén preparados para hacerles frente. El 39% de las instituciones sanitarias no sabe cómo protegerse contra estas amenazas.

3.2. Aspectos a solucionar

Para mejorar la percepción de seguridad al interior de la empresa Keralty, se debió minimizar los incidentes cibernéticos derivados de la mala administración que tenían los firewalls y que habían ocasionados ataques a la infraestructura tecnológica de la empresa, pero sin repercusiones a gran escala, sin embargo, si se hubiera continuado por el mismo camino, es decir, haciendo caso omiso a las alertas que ya se habían generado, los riesgos serian altos. Por tal motivo, fue indispensable cerrar los agujeros de seguridad causados por el firewall y la falta de capacitación y conciencia de los empleados en seguridad de la información, para contribuir a un ambiente seguro al interior de la empresa.

Según el artículo científico "Entorno para Experimentación de Vulnerabilidades en la Enseñanza de Buenas Prácticas de Programación" por Uri Yael y Benjamín Barán, los buenos resultados y disminución de brechas en vulnerabilidades cibernéticas recae sobre una actualización de personal con mentalidades renovadas y salir del trabajo cotidiano tradicional que es el mismo que viene generando miles de puertas abiertas para los atacantes.

De igual manera, aunque no es un aspecto a solucionar porque aún no está implementado, si es importante mencionar que se adicionara un Sistema de Prevención de Intrusos (IPS) para reforzar la seguridad de la red de la empresa. Además, de la actualización del antivirus y de la mencionada capacitación de seguridad a los usuarios que recibirán por los integrantes del presente proyecto; esto último, en el entendido que nunca han recibido orientación profesional en seguridad de la información por el personal de la empresa.

Aquellos aspectos a solucionar con relación a los firewalls y servidores son:

- La configuración de las reglas actuales de los firewalls que están permitiendo tráfico con orígenes y destinos all.
- Se ha identificado que no se cuenta con un formato para los requerimientos de creación, modificación o eliminación de reglas en el firewall, lo que significa que no está documentado la configuración de este dispositivo de seguridad.
- Los firewalls no cuentan con perfiles de webfilter y application control debidamente configurados, ocasionado accesos no autorizados por los usuarios.
- No se cuenta con la herramienta para realizar informes de consumo de servicios, verificación de tráfico, entre otras funcionalidades, que permitan tener control de la red de Keralty. Para lo anterior, se está gestionando la herramienta fortianalyzer.
- Tomar acciones correctivas de configuración y software sobre los aplicativos expuestos en los servidores de acuerdo con las recomendaciones brindadas en el informe técnico.

3.3. Solución propuesta

Se aprovechó al máximo posible los recursos que brinda el firewall, lo que indica que se configuraron reglas agrupadas en el firewall, con el fin de tener más orden, mayor alcance y asignación de herramientas y permisos estrictamente necesarios a los empleados de la compañía. Adicional se implementarán nuevas herramientas como IPS, Fortianalyzer, actualización de

licencias, actualización de antivirus, implementación de formatos (basados en ITIL) y capacitación constante a los empleados sobre pautas de seguridad.

Se generará informe técnico de análisis de vulnerabilidades aplicado directamente al área de servidores en ambiente de preproducción, se detallara falla, causa y posible solución que quedara en manos del director de infraestructura quien tomara la decisión de aplicar las correcciones o no.

4. Estado del arte

4.1. Marco de referencia teórico

La seguridad de redes telemáticas trata de asegurar la información que se almacena y viaja a través de las redes, pero antes de hablar de los mecanismos de seguridad que utilizaremos para este proyecto, es necesario conocer y precisar el concepto básico de la seguridad que según Bosworth, Kabay y Whyne descrito en su libro Computer Security Handbook, la definen como el estado de estar libre de peligro y no expuesto a los daños causados por accidentes o ataques. Además, expresan que el objetivo de un sistema de seguridad de la información, es mejorar el rendimiento de una organización con respecto a las amenazas y riesgos a los que está expuesta, buscando asegurar y proteger la disponibilidad, integridad y confidencialidad de la información.

Este proyecto se enfoca en identificar y mejorar las políticas de firewall interno de la empresa Keralty a fin de reducir los riesgos asociados, como la navegación libre a Internet de los clientes, entre otros, además, de realizar el escaneo de vulnerabilidades a los servidores de preproducción y posterior proponer soluciones con base a estos escaneos y a las mejores prácticas de seguridad que ofrece la industria.

1. FIREWALL

La seguridad no fue uno de los principios en el diseño de las redes y protocolos entre los 60s y 70s, razón por la cual se han venido desarrollando tecnologías de software y hardware para añadirles una capa de seguridad de la que carecían, uno de los componentes ha sido el firewall, que han venido evolucionando en términos de complejidad y efectividad.

Un firewall es un dispositivo que funciona entre redes, permitiendo o denegando las comunicaciones de una red a la otra. Uno de sus usos típicos es situarlo entre una red corporativa interna y la red Internet, como un dispositivo de seguridad para prevenir que los intrusos puedan

acceder a la información empresarial. También es frecuente conectar al firewall una tercera red, llamada DMZ, en la que se ubican los servidores de la organización que deben ser accesibles desde la red exterior. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad.

Un firewall filtra las comunicaciones que pasan de una red a otra, permitiendo o denegando su tráfico, es decir, examina el tipo de servicio al que corresponde, como puede ser correo, web, ftp, etc., además que valida si la comunicación es entrante o saliente dependiendo de su dirección para permitirla o no, en este orden de ideas, un firewall puede permitir desde una red local hacia Internet servicios de correo, web, ftp, pero no a IRC que puede ser innecesario para el trabajo.

Hay dos políticas básicas en la configuración de un firewall para la seguridad en la organización:

- ✓ Política restrictiva: Denegando todo el tráfico, habilitando expresamente el tráfico de los servicios que se necesitan.
- ✓ Política permisiva: Permitiendo todo el tráfico excepto los servicios potencialmente peligrosos que necesitan aislarse.

La política restrictiva es la más segura, debido a que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya previsto tráfico peligroso y sea permitido por omisión.

Algunas de las preguntas fundamentales que debe responder cualquier política de seguridad son [3]:

- ✓ ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).

- ✓ ¿De quién proteger? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.
  Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios y denegando cualquier tipo de acceso a otros.

- ✓ ¿Cómo proteger? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización, puede optarse por alguno de los siguientes paradigmas o estrategias:
  a. Paradigmas de seguridad
     - Se permite cualquier servicio excepto aquellos expresamente prohibidos.
     - Se prohíbe cualquier servicio excepto aquellos que están permitidos.
  b. Estrategias de seguridad
     - Paranoica: Se controla todo, no se permite nada.
     - Prudente: Se controla y se conoce todo lo que sucede.
     - Permisiva: Se controla, pero se permite demasiado.
     - Promiscua: No se controlada (o se hace poco) y se permite todo.

- ✓ ¿Cuánto será su costo? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.

De otro lado, los firewalls no deben ser la única solución para la seguridad de la información, pero si es considerado una parte integral de defensa dentro de la estrategia de seguridad de la red. Este componente sino se administra e implementa correctamente, puede dejar brechas de seguridad que pueden permitir a los criminales entrar y salir de la red empresarial, además que la mala manipulación del mismo, podría dejar sin acceso a un servidor critico desde parte de la red. Todas las redes son diferentes, y no hay ninguna solución para crear una configuración de firewall a prueba de hacker, pero lo que si hay son recomendaciones o mejores prácticas para administrar un firewall de red. Algunas de las mejores prácticas son [4]:

- ✓ Denegar todo el tráfico de manera predeterminada, y dejar solo habilitado aquellos servicios que son necesarios.
- ✓ Deshabilite o desístale cualquier servicio o software innecesario en el firewall.
- ✓ Cambie el administrador de firewall predeterminado o la contraseña de root.
- ✓ Asegúrese de que está filtrando los paquetes para las direcciones correctas según el Top 20 de SANS llamado "Not filtering packets for corrects incoming and aoutgoing addresses".
- ✓ Asegúrese de que está filtrando o deshabilitando todos los puertos innecesarios y

los puertos vulnerables comunes basado en el Top 20 de SANS llamado "Large number of open ports and common vulnerable ports".

- ✓ Mantenga la configuración de su firewall lo más simple posible y elimine reglas innecesarias o redundantes para garantizar que el firewall este configurado para satisfacer sus necesidades específicas.
- ✓ Actualice el sistema operativo y el software de la aplicación del software con el último código de forma regular.
- ✓ Configure el acceso adecuado a la administración remota.
- ✓ Crear un comité de control de cambios en el firewall.
- ✓ Alertar a usuarios y administradores de sistemas antes de realizar cambios en las reglas del firewall.
- ✓ Documentar todas las reglas y utilizar los comentarios para explicar el propósito de las reglas.
- ✓ Controle regularmente los registros del firewall.
- ✓ Realice evaluaciones de vulnerabilidades en el firewall de forma continua para probar fallas y debilidades de software.
- ✓ Supervise o suscríbase a los boletines de seguridad de su proveedor.

Cabe anotar que cada proveedor de firewall e institutos de seguridad a nivel mundial como SANS y NIST proporcionan criterios semejantes, pero no iguales en mejores prácticas de seguridad para los firewalls, por eso es importante probar los cambios importantes en un entorno que no sea de producción para asegurar su funcionalidad.

2. SERVIDORES

Keralty como muchas de las empresas del sector salud, ha sido blanco de diversos ataques informáticos que buscan poder acceder a los servidores, sistemas e información confidencial, con el propósito de sabotear, alterar y manipular los datos para beneficios lucrativos. En años recientes se había reportado un incremento en ataques informáticos a esta empresa alertando a los administradores de la infraestructura TI sobre los serios problemas de indisponibilidad de la información y credibilidad de imagen a los que estaba expuesta esta entidad de la salud a diario.

El análisis de vulnerabilidades el cual es una parte del proceso de análisis de riesgo, es una actividad fundamental orientada hacia un sistema de gestión de la seguridad de la

información, el cual comprende las siguientes actividades [5]:

1. Entendimiento de la infraestructura.

En esta fase se buscó identificar cada uno de los dispositivos de hardware que componen la infraestructura y que soportan los procesos del negocio. Dentro de estos elementos de la infraestructura que tenían vulnerabilidades eran los servidores de preproducción que eran nuestro material de estudio, dejando a un lado los demás activos TI de la empresa, pero entendiendo que seguramente los demás activos también tenían vulnerabilidades.

2. Pruebas.

Se realizó una clasificación de activos o dispositivos según la importancia del mismo para la continuidad del proceso en estudio. Ahora, por medio de herramientas para la detección de vulnerabilidades, soportadas por su fabricante y que cuenten con una base de datos actualizada y completa de vulnerabilidades, además con un criterio común de clasificación como el CVE, se identificaron el rango de dirección IP de los servidores, con el propósito de detectar sus vulnerabilidades presentes a nivel de software y así evitar futuros incidentes de seguridad.

3. Medidas preventivas.

Una vez seleccionadas las herramientas y los activos, se debieron tomar medidas preventivas para su ejecución, con el fin de prevenir efectos adversos sobre la prestación de servicios, entre las que podemos resaltar:

- ✓ Definir hora adecuada de pruebas.
- ✓ Realizar un análisis de riesgo cualitativo sobre la prueba.
- ✓ Tomar algunas medidas de contingencia.
- ✓ Realizar monitoreo de los servicios durante las pruebas.
- ✓ Informar a los dueños de los activos.

4. Realización de las pruebas de vulnerabilidades.

El tiempo varía según la cantidad de IP’s a escanear, y las pruebas se pueden ser internas o externas y sin conocimiento o con conocimiento de los activos. Para nuestro caso, este escaneo no excedió los 30 minutos y se debió solicitar autorización para realizar las pruebas internas de

los servidores.

5. Pruebas de explotación de las vulnerabilidades.

Luego de obtener las vulnerabilidades más críticas, se debe realizar una prueba sobre ellas con el fin de realizar su explotación, que incluye el escalar privilegios (no se realizó en el presente proyecto).

6. Análisis de resultados.

Con base a la información obtenida se realizó una reunión técnica para informar de estos resultados para tomar decisiones.

7. Plan de remedición de vulnerabilidades.

Por último, establecer un plan de remediación para las vulnerabilidades encontradas a través de controles tecnológicos o administrativos que le corresponde al administrador de los servidores de Keralty.

4.2. Marco de referencia tecnológico

Establecer normas que minimicen cualquier riesgo a la información contenida, infraestructura computacional y por supuesto a los usuarios, es el objetivo de la seguridad informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización además de velar que los equipos funcionen adecuadamente, proveer planes de contingencias, asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la información [6]. Lo anterior, con el fin de asegurar que los recursos y el acceso a estos sean realizados de manera correcta, llevando un seguimiento a las modificaciones y consultas de dicha información asegurando que estas sean realizadas solo por usuarios autorizados. Por esta razón, la seguridad de la infraestructura y aplicaciones debe estar incorporada desde el diseño, garantizando la evaluación de los factores funcionales y técnicos a tener en cuenta para el uso seguro del entorno. Si esto sucede, el objetivo inicial de la seguridad se habrá cumplido.

Las soluciones preventivas y correctivas que se implementen en Keralty, ya sea solo con el personal interno o con la ayuda de una empresa que ofrezca servicios de pruebas de vulnerabilidad y test de intrusión, como por ejemplo, NetData Network, B Secure, Ecomil, InformationTechnology Security Solutions (ITSS) Ltda, entre otras, deben garantizar el equilibrio entre el costo que tiene la resolución de la vulnerabilidad, el valor del activo de información para la empresa y el nivel de criticidad de la vulnerabilidad. Además, el escaneo de vulnerabilidades externas e internas junto con las medidas correctivas da confianza a los clientes sobre sus datos y da una ventaja competitiva a la empresa al fortalecer de manera anticipada su entrono frente a posibles amenazas [7].

En nuestro caso, se realizaron correcciones a nivel de firewall perimetral y se evaluaron vulnerabilidades existentes sobre los servidores preproducción de la compañía, estas funciones se realizaron utilizando las siguientes herramientas tecnológicas con la intervención del personal interno de la empresa.

FORTIGATE

Es un Firewall basado en hardware desarrollado por Fortinet. El sistema de FortiGate es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. Las soluciones de FortiGate también incluyen: firewall, filtrado de contenido, VPN, antivirus, antispam, Detección y prevención de intrusos y gestor de tráfico, balanceo de carga y alertas por e-mail [8].

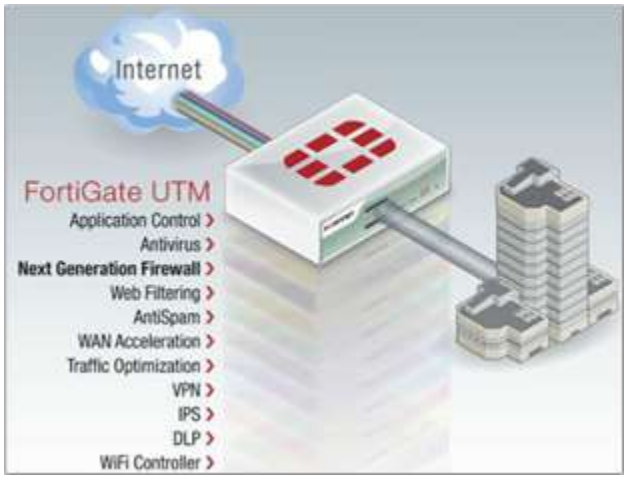


Figura 2: Soluciones de seguridad de FortiGate UTM.

NESSUS

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

En operación normal, Nessus comienza escaneando los puertos con Nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades [9].

Figura 3: Comparación de herramientas para la evaluación de vulnerabilidades de aplicaciones.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

NMAP

Nmap ("Network Mapper") es una fuente gratuita y de código abierto utilizada para el descubrimiento de redes y auditorías de seguridad. A muchos administradores de sistemas y redes también les resulta útil para tareas como el inventario de redes, la administración de programas de actualización de servicios y la supervisión del tiempo de actividad del host o del servidor. Nmap utiliza paquetes de IP sin procesar en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre de aplicación y versión) ofrecen, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y docenas de otras características [10].

5. Glosario de términos

Activo de información

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

Según el ISO 17799:2005 (Código de práctica para la gestión de seguridad de información), un activo de información es algo a lo que una organización directamente le asigna.

Amenaza

Los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado, que puede generar daño a la organización y a sus activos. Una amenaza es la indicación de un potencial evento no deseado.

Las amenazas se pueden clasificar en:

Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).

Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas).

Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).

Confidencialidad

La confidencialidad es la propiedad para prevenir la divulgación de información a personas o sistemas no autorizados. La pérdida de la confidencialidad de la información puede acoger muchas formas.

Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Para los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad en sistemas tiene como objetivo estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

La disponibilidad además de ser importante en el proceso de seguridad de la información es, además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web, etc.; mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

Firewall

Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

FortiAnalyzer

Ofrece registro e informes de seguridad de red centralizados, proporciona alertas en tiempo real que agilizan el descubrimiento, la investigación y la respuesta a los eventos, incluso mientras ocurren. Con vistas consolidadas orientadas a la acción y capacidades de exploración profunda, FortiAnalyzer ofrece a las organizaciones una visión completa de las amenazas que se producen en toda la superficie de ataque. También proporciona inteligencia de amenazas en tiempo real y análisis accionables a través de comprobaciones de alimentación de IOC globales para detectar amenazas emergentes y recientes en toda la organización. En esta demostración, verá todas estas capacidades.

Integridad

La Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando alguna persona modifica o borra los datos importantes.

IPS

Un Sistema de Prevención de Intrusos (o por sus siglas en ingles IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Política de seguridad

Son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. La política de seguridad forma parte de la política general y debe ser aprobada por la alta dirección.

La Política de seguridad de una empresa es un documento auditable ya sea por los auditores internos de la empresa o por externos en busca de una certificación, inclusive por el cliente. Por este motivo este documento debe ser entendido a todos los niveles, desde el personal operativo / operador hasta los altos mandos (directores, gerentes, etc.).

Una política de seguridad es como la "carta de presentación de la empresa" donde se

exponen los puntos que quiere dar a conocer la empresa, ¿a qué se dedica?, ¿qué quiere lograr?, ¿bajo qué método trabaja?, ¿Cómo lo quiere lograr? estas cuatro preguntas son la estructura que debe llevar la carta de presentación ante el cliente, el quien al leer estos cuatro puntos va a tener una idea muy clara de la empresa a la que está a punto de comprar sus productos o servicios. Existen cuatro pasos esenciales para lograr un fácil entendimiento y estructuración de una política de seguridad.

Servidor

Equipo de cómputo diseñado con arquitectura de altas especificaciones en capacidad y rendimiento, encargado de proveer a una serie de clientes diferentes servicios, tales como administración de bases de datos, servicios HTTP, repositorios, etc.

Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Riesgo residual

Es el riesgo remanente después de haber realizado el tratamiento del riesgo.

Seguridad de información

La seguridad de la información son todas aquellas medidas preventivas y reactivas que los administradores de TI, que permiten que la información sea protegida para mantener la disponibilidad e integridad de la misma proteger la confidencialidad.

En la seguridad de la información es importante mencionar que su manejo está basado en la tecnología y debemos realizar una clasificación de la información para catalogarla como confidencial, puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc.

Vulnerabilidad

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. Las vulnerabilidades pueden clasificarse como:

Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimientos que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).

Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para el control de acceso, passwords sin modificarse).

Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, susceptibilidad de equipos a variaciones de voltaje).

6. Justificación

En la organización Keralty se está presentando un alto índice eventos de seguridad de la información en las diferentes áreas, por tanto, se debió revisar las malas prácticas que se estaban ejecutando y realizar un escaneo de vulnerabilidades para presentar un informe o un indicador sobre el riesgo en el que se encontraba la protección de los datos.

A lo anterior fue preciso diseñar un proyecto de aseguramiento y afinamiento de la configuración del firewall e implementar servicios de seguridad como antivirus, IPS (Sistema de Prevención de Intrusos), dispositivo de análisis de tráfico como un fortianalyzer y desarrollar mecanismos que ayuden a mitigar impactos de la seguridad de la información, puesto que éstos pueden ser puntos críticos para el desarrollo de las actividades de la organización Keralty.

Los servidores de iWeb se entregan sin administración, excepto las ofertas de alojamiento administrado donde algunas partes de la seguridad de la infraestructura de TI están incluidas en el paquete. Como tal, la protección de los servidores se considera responsabilidad del cliente, La preocupación principal al momento de activar y poner en marcha una aplicación es al momento de

configurar la infraestructura. Sin embargo, el tener una aplicación que es funcional, pero que no tiene en cuenta las necesidades de seguridad asociadas a la infraestructura que se está utilizando, podría acarrear consecuencias devastadoras, provenientes de atacantes que utilicen técnicas simples y de bajo esfuerzo para identificar y explotar vulnerabilidades, ya que no se realizan verificaciones se seguridad a las aplicaciones en la empresa.

7. Objetivos

7.1 General

Identificar y proponer una solución de mejora a las vulnerabilidades informáticas presentes de la red y del ambiente de servidores de preproducción de la entidad Keralty.

7.2 Específicos

1. Entregar un informe del comportamiento del módulo de IPS activo en el FW de los meses de abril, mayo y junio, para identificar tendencias de ataques y las contramedidas aplicadas a estas.
2. Depurar la configuración de las políticas actuales del firewall de producción con base a los perfiles de webfilter y application control.
3. Realizar pruebas a los servidores del área de preproducción que permitan diagnosticar y evaluar las vulnerabilidades encontradas.
4. Analizar las vulnerabilidades más críticas encontradas en los servidores de preproducción de Keralty.
5. Entregar un documento con recomendaciones, según el análisis de vulnerabilidades hechas a los servidores.

8. Requerimientos

A continuación se presentan los requerimientos de este proyecto por fase:

Fase 1 (Estudio inicial)

1.1 Analizar el estado actual de la compañía, identificar sus recursos y cómo es su estructura tecnológica.

1.2 Asimilar el negocio de la compañía, con el fin de encontrar sistemas críticos y que

necesiten una especial atención.

1.3 Estudiar el organigrama de la compañía, determinar los responsables de los sistemas que se van a evaluar y conocer su funcionamiento los procedimientos de los recursos tecnológicos de la compañía.

1.4 Agrupar documentos en donde se expliquen políticas, procesos y procedimientos que vayan apuntados a la seguridad informática y de la información en la compañía.

Fase 2 (Planear actividad)

2.1. Identificar y aclarar el alcance que la compañía permita para realizar un escáner de vulnerabilidades y equipos que permitan ser evaluados y corregidos.

2.2. Seleccionar las herramientas que se van a usar para la identificación de vulnerabilidades en todos los sistemas previamente seleccionados.

2.3. Establecer un cronograma de actividades que no afecten la actividad del negocio.

2.4. Presentar el cronograma de actividades a la empresa con el fin de obtener su consentimiento.

Fase 3 (Ejecutar actividad)

3.1. Realizar análisis preventivos, basados en guías de hardening sobre firewall existente en la compañía.

3.2. Aplicar plan correctivo sobre firewall Fortigate con estándar de buenas prácticas.

3.3. Realizar la instalación de herramientas de identificación de vulnerabilidades en un ambiente controlado, sin riesgo de afectar el negocio y que sea aprobado por la empresa.

3.4. Ejecutar el cronograma de actividades de identificación de vulnerabilidades en los sistemas previamente seleccionados.

3.5. Realizar pruebas a los servicios afectados, con el fin de comprobar su correcto funcionamiento.

3.6. Recopilar toda la información y resultados de las herramientas usadas para la identificación de vulnerabilidades.

Fase 4 (Análisis de resultados)

4.1. Identificar todas las vulnerabilidades críticas encontradas en la fase de escáner.
4.2. Investigar el impacto de las vulnerabilidades encontradas en los sistemas críticos del negocio.
4.3. Determinar cuáles son las soluciones viables a las vulnerabilidades críticas o como se pueden mitigar.

Fase 5 (Entrega de resultados)

5.1. Elaborar un documento donde se expongan los resultados del análisis efectuado en la fase anterior.
5.2. En el documento sobresalen las vulnerabilidades críticas que tengan una mayor probabilidad de ocurrencia y tengan el potencial de afectar seriamente al negocio.
5.3. El documento elaborado contiene recomendaciones hacia la empresa para reforzar su seguridad y prevenir un impacto negativo al negocio.

9. Metodología de desarrollo

Para llevar a cabo la depuración de las políticas actuales del firewall y el análisis de vulnerabilidades a los servidores de preproducción de Keralty, se planeó realizar un proceso con una metodología propia de los autores, basada en la experticia de trabajo a lo largo de los años, la cual está dividida por fases como se detalla a continuación.

9.1. Fases del proyecto de grado

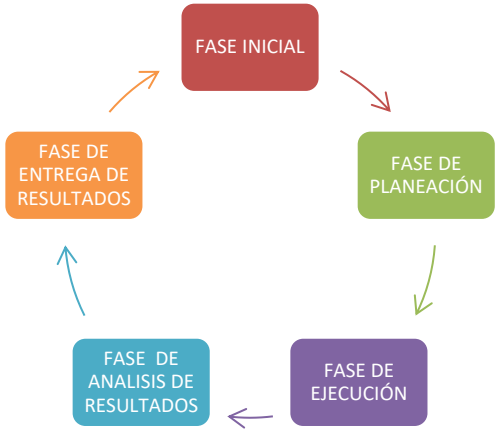


Figura 4: Metodología de desarrollo.

1. FASE INICIAL

En esta fase se realizó el levantamiento de información necesaria para el cumplimiento de los objetivos planteados, definiendo los activos de TI junto con su topología de red, direccionamiento IP, políticas de enrutamiento, perfiles de navegación, estado de canales de Internet, nombres de equipos, principales servicios, responsables de los activos, entre otra información que fue útil para el desarrollo del proyecto.

2. FASE DE PLANEACION

En esta fase se estableció un plan de trabajo en donde se definió con claridad el alcance, las tareas que se tenían que realizar, los entregables y los requisitos de los mismos, los recursos necesarios y un cronograma de tareas que se necesitaron para realizar la depuración de las políticas del firewall y del análisis de vulnerabilidades de los servidores de preproducción.

3. FASE DE EJECUCION

Se ejecutaron los mecanismos necesarios para depurar las políticas del firewall y se identificaron la mayor cantidad de las vulnerabilidades en los servidores, además estas se evaluaron para brindar un documento con las mejores prácticas de configuración, ofreciendo así, una mayor seguridad de la información al evitar ataques malintencionados por parte de terceros.

4. FASE DE ANALISIS DE RESULTADOS

En esta fase se tomaron como base los resultados de la fase anterior, para recopilar y estudiar las vulnerabilidades más críticas para conocer su impacto y brindar las mejores opciones para dar solución a los problemas de los servidores. Además, en cuanto al firewall, se probaron las nuevas políticas configuradas que ayudarían a cerrar agujeros de seguridad en la red.

5. FASE DE ENTREGA DE RESULTADOS

Se procedió a elaborar un documento final que dan a conocer al jefe del área de TI los resultados de las actividades realizadas a través de un informe con las nuevas políticas del firewall y de las vulnerabilidades encontradas, sustentando su impacto y motivando a Keralty a corregir los hallazgos en un corto plazo.

9.2. Instrumentos o herramientas utilizadas

Como técnicas e instrumentos para llevar a cabo el desarrollo de los objetivos se tuvieron en cuenta entrevistas, análisis de documentos y la observación directa, que sirvieron para el levantamiento de información de la información, caracterización de activos y ejecución de las actividades a desarrollar.

9.2.1. Entrevista

Este es un instrumento directo para el levantamiento de información en reuniones programadas con la asistencia del personal administradores, usuarios de sistemas de información y de recursos tecnológicos en general; con el propósito que nos suministraran información de los servidores con los que se cuenta, así mismo, los riesgos informáticos a los que estaban expuestos y de conocer sus opiniones frente a la importancia de proteger y de utilizar de manera adecuada los recursos informáticos.

De igual manera, se hizo uso de la entrevista dirigida mediante una serie de encuestas; a fin de poder obtener mayor cantidad de información precisa y valida que facilitaron la identificación de posibles fallas, vulnerabilidades y aspectos por mejorar que rodean el uso de los recursos tecnológicos dentro Keralty.

9.2.2. Análisis de documentos

Se estudiaron los documentos necesarios que tenía Keralty, que ayudaron a conocer repositorios de archivos, software, bases de datos, fichas técnicas, auditorias y demás información que fue necesaria del firewall y de los servidores de preproducción.

9.2.3. Observación directa

Este instrumento consistió en observar atentamente el caso en estudio, tomar información y registrarla para su posterior análisis. Para el desarrollo del presente proyecto, se realizaron visitas guiadas por el administrador de los servidores, lo que permitió tomar evidencia fotográfica y visual del estado actual de los recursos técnicos y tecnológicos, su organización, utilización y de los demás elementos que intervienen en el desarrollo normal del core del negocio de la empresa.

9.2.4. Herramientas de seguridad informática

NESSUS: Es el escáner de vulnerabilidades más popular y utilizado en las organizaciones en todo el mundo. Muchas organizaciones están utilizando Nessus como herramienta de auditoria de sistemas de información para la búsqueda de fallas criticas de seguridad.

NMAP: Es una herramienta gratuita de código abierto para la exploración de la red o la auditoria de seguridad.

10. Capítulos de desarrollos

Para el desarrollo del proyecto se han realizado las siguientes actividades:

10.1. Contexto

Sanitas nace en España centrando su actividad en el sector de la salud, los primeros pasos de Sanitas Internacional en Latinoamérica fueron en Colombia, con la creación de la compañía de Asistencia Médica ColSanitas, estableciendo en el país un novedoso modelo de aseguramiento privado voluntario denominado Medicina Prepagada. Esto supuso el primer paso para la creación de un hospital y de una estructura administrativa que, actualmente, está presente en todo el país, ColSanitas abre su primera clínica en Colombia. Actualmente, Clínica ColSanitas es una de las mayores redes privadas de salud en Colombia. EPS Sanitas surge como respuesta al sistema colombiano de Seguridad Social con el fin de garantizar la atención establecida en el Plan Obligatorio de Salud (Ley 100/1993). Para cumplir con los servicios incluidos en dicho plan, EPS Sanitas ha desarrollado una extensa red de médicos afiliados, tecnología e infraestructura que constituyen un área médica extendida a lo largo de todo el país. La creación de la Fundación Sanitas constituye el nacimiento de una institución sin ánimo de lucro dedicada a la mejora de las condiciones de vida de las personas más desfavorecidas. Sanitas Internacional llega al sector de la medicina prepagada ofreciendo, entre otros, cobertura en consultas médicas externas de las especialidades, hospitalización, maternidad y cirugía (programada y de emergencia); acceso a CliniSanitas, Odontosanitas, Oftalmosanitas y Farmasanitas y consulta médica y hospitalización a domicilio.

La Organización Sanitas Internacional ahora es Keralty, derivada del término 'care' (del verbo inglés 'cuidar'), la nueva marca Keralty nace como símbolo de una gestión en salud

moderna, profesional e integradora, capaz de conjugar una presencia global con una atención única y personalizada, siempre adaptada a las necesidades de cada paciente.

De otro lado, para desarrollar este proyecto se realizó una solicitud de permiso a los Directores del Centro de Cómputo de Keralty y del Administrador de los Servidores para socializarles el proyecto que se quería proponer en la Universidad El Bosque como trabajo de grado, exponiendo la problemática interna del firewall y de los servidores de preproducción de la empresa, pero que ayudaran a conocer en detalle las falencias de estos activos para luego cerrar los agujeros de seguridad. Lo anterior fue aprobado y apoyado por parte de la empresa.

10.2. Planeación

Una vez planteado y teniendo la aprobación del director de infraestructura de Keralty para la ejecución se realiza un levantamiento de información con él fin de mapear el estado actual del uso vs buenas prácticas del firewall perimetral. Se ejecutan mejoras a nivel firewall perimetral guiados por guía de hardening brindado por fabricante.

Se realiza análisis a los servicios del ambiente de preproducción con herramientas de disección de vulnerabilidades, con dicha información levantada se realiza el diagnósticos pasando a la fase de análisis y la planeación del proyecto, también se identifican los servicios críticos y a partir de esto se realiza la fase de diagnóstico, posteriormente se realiza la fase de análisis de vulnerabilidades encontradas junto con la presentación de conclusiones y finalmente la formulación del plan de mejoras.

10.3. Ejecución

La ejecución de tareas se llevará acorde al cronograma de actividades, el objetivo de este proyecto concadena varias actividades para lograr el entregable. Con dichas tareas se permitirá definir los servicios y equipos que fueron objeto de este análisis de vulnerabilidades y el alcance critico de las herramientas objeto de este proyecto junto con la implementación de buenas prácticas sobre firewall perimetral

Identificada la topología implementada en Keralty se procede a establecer ciertos objetivos catalogados como los más relevantes (servidores preproducción) a los cuales se les

realizarán los escaneos de vulnerabilidades y pruebas a ejecutar en el desarrollo de este proyecto.

10.4. Análisis

Durante el análisis se realizan las actividades incluidas en el cronograma con el fin corregir malas prácticas en firewall perimetral e identificar las vulnerabilidades de seguridad sobre servidores de preproducción de la empresa Keralty y definir su estado actual. Los objetivos seleccionados dentro de la organización para realizar las pruebas de vulnerabilidades son principalmente servidores, estas pruebas se llevan a cabo con una serie de herramientas de software gratuito utilizados para identificar vulnerabilidades tales como NMAP y NESSUS mediante las cuales es posible realizar un reconocimiento activo de la red, en donde se identifica puertos abiertos, servicios asociados y vulnerabilidades conocidas.

10.4.1. Firewall

A. Módulo de IPS activo en el FW

Los eventos e incidentes de seguridad presentados hacia la infraestructura protegida de Keralty, más recurrentes identificados por medio del módulo IPS activo en el firewall interno de los meses de abril, mayo y junio son los siguientes:

1. Análisis eventos trimestral

En la siguiente figura se especifica los ataques detectados por el IPS.

Mes	Cantidad
Abril	7868
Mayo	4986
Junio	3336
Total	**16190**

Figura 5: Número de ataques detectados por IPS (abril-junio)

De acuerdo a las estadísticas anteriores, se presenta una tendencia de disminución a los eventos del segundo trimestre del presente año, lo cual el IPS realiza las siguientes acciones a los 16190 eventos detectados:

Severidad	Acción	Cantidad Ataques	%
Critical	Detected	1	0%
Critical	Dropped	941	100%
High	Dropped	924	6%
High	Dropped	14315	94%
Medium	Dropped	9	100%
Total		**16190**	

Tabla 1: Acciones a eventos detectados

Las categorías HIGH y CRITICAL el IPS Dropped a más del 90% de los paquetes.

2. Top Eventos Origen/Destino

Se realiza una depuración de eventos dejando solo aquellos eventos los cuales presentan un comportamiento predecible y/o recurrente.

En la siguiente tabla se observa la identificación del TOP 10 de los eventos, que presentan el 90% del total reportado por el IPS lo cual se atribuye que son 16190 eventos detectados.

Ataques	Cantidad
HTTP.URI.SQL.Injection	13806
MS.RDP.Connection.Brute.Force	925
Apache.Struts.2.Jakarta.Multipart.Parse r.Code.Execution	331
Red.Hat.Jboss.AS.doFilter.Insecure.Deserialization	210
Jboss.JMX.Console.Beanshell.Deployer. War.Upload	185
OpenSSL.Heartbleed.Attack	164
HTTP.Request.URI.Directory.Traversal	128
Jboss.JMX.Console.Beanshell.Deployer.War.Upload	98
Apache.Commons.Colletion.InvokerTrans former.Code.Execute	72
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execute	56
Total	**15975**

Tabla 2: TOP 10 de eventos detectados

3. Comportamiento de ataques

Los ataques detectados por el IPS corresponden en la mayoría de casos a patrones ya conocidos, por lo tanto, estos son bloqueados por el módulo de IPS mediante el reconocimiento de los mismos.

A continuación, los vectores de ataque y mitigaciones realizadas para los eventos con mayor número de intentos de ataques en el TOP 10 presentado anteriormente.

3.1. Evento y comportamiento HTTP.URI.SQL.Injection

Los eventos de inyección SQL indican un intento de explorar una vulnerabilidad de SQL a través de solicitudes HTTP. La vulnerabilidad es el resultado de la falla de la aplicación para verificar la entrada proporcionada por el usuario antes de usarla en una consulta SQL. Como resultado, un atacante remoto podría enviar una consulta elaborada para ejecutar comandos SQL no autorizados en un servidor vulnerable. Cualquier aplicación web puede estar afectada por este tipo de ataque, la recomendación más asertiva para este tipo de eventos es tener actualizada a la última versión el software para la publicación de la página web.

Ataques	Srcip	Dstip	Dstport	Cantidad Ataques
HTTP.URI.SQL.Injection	80.211.244.195	172.22.150.66	80	2803
HTTP.URI.SQL.Injection	54.38.155.44	172.22.150.66	80	1852
HTTP.URI.SQL.Injection	173.63.70.157	172.22.150.66	80	1390
HTTP.URI.SQL.Injection	35.196.151.79	172.22.150.66	80	1390
HTTP.URI.SQL.Injection	47.90.246.81	172.22.150.66	80	807
HTTP.URI.SQL.Injection	47.89.255.152	172.22.150.66	80	795
HTTP.URI.SQL.Injection	35.196.104.147	172.22.150.66	80	794
HTTP.URI.SQL.Injection	27.254.81.219	172.22.150.66	80	438
HTTP.URI.SQL.Injection	112.78.5.70	172.22.150.66	80	410
HTTP.URI.SQL.Injection	108.174.200.241	172.22.150.66	80	188
HTTP.URI.SQL.Injection	1.234.36.9	172.22.150.66	80	161
HTTP.URI.SQL.Injection	81.169.144.135	172.22.150.66	80	100
HTTP.URI.SQL.Injection	131.255.158.226	172.22.150.66	80	96
HTTP.URI.SQL.Injection	206.189.74.226	172.22.150.66	80	93
HTTP.URI.SQL.Injection	5.62.47.40	172.22.150.66	80	93
HTTP.URI.SQL.Injection	177.71.67.7	172.22.150.66	80	90
HTTP.URI.SQL.Injection	190.39.121.113	172.22.150.66	80	90
HTTP.URI.SQL.Injection	177.47.27.209	172.22.150.66	80	85
HTTP.URI.SQL.Injection	195.201.29.170	172.22.150.66	80	84

HTTP.URI.SQL.Injection	103.67.235.109	172.22.150.66	80	83
HTTP.URI.SQL.Injection	50.77.222.138	172.22.150.66	80	74
HTTP.URI.SQL.Injection	94.247.31.203	172.22.150.167	80	72
HTTP.URI.SQL.Injection	104.196.23.50	172.22.150.66	80	71
HTTP.URI.SQL.Injection	185.222.201.21	172.22.150.66	80	68
HTTP.URI.SQL.Injection	103.59.59.6	172.22.150.66	80	66
HTTP.URI.SQL.Injection	190.40.237.214	172.22.150.66	80	64
HTTP.URI.SQL.Injection	85.59.59.6	172.22.150.66	80	62
HTTP.URI.SQL.Injection	212.7.63.17	172.22.150.66	80	60
HTTP.URI.SQL.Injection	35.196.230.103	172.22.150.66	80	60
HTTP.URI.SQL.Injection	157.192.230.154	172.22.150.66	80	54
Total				**13806**

Tabla 3: Eventos de inyección SQL mediante solicitudes HTTP

3.2. Evento y comportamiento MS.RDP.Connection.Brute.Force

El ataque consiste en múltiples solicitudes de RDP destinadas a realizar un inicio de sesión RDP por fuerza bruta, lanzado a una velocidad de aproximación 200 veces en 10 segundos. Generalmente este tipo de ataques se presenta en el protocolo remoto de Microsoft, se recomienda ajustar el umbral de la red para evitar este tipo de ataques, ya que este comportamiento es reiterativo; adicionalmente esta vulnerabilidad está asociada a intentos de conexión desde Internet al puerto RDP 3389, por lo cual se recomienda validar si es necesario tener publicado este puerto, en caso contrario se debe cerrar l filtrar una cantidad limitada de IP's.

Ataques	Srcip	Dstip	Dstport	Cantidad Ataques
MS.RDP.Connection.brute.Force	139.60.160.150	172.18.48.154	3389	1
MS.RDP.Connection.brute.Force	177.221.246.3	172.18.48.154	3389	789
MS.RDP.Connection.brute.Force	181.48.26.180	172.18.48.154	3389	2
MS.RDP.Connection.brute.Force	185.222.209.31	172.18.48.154	3389	10
MS.RDP.Connection.brute.Force	217.12.57.132	172.18.48.154	3389	3
MS.RDP.Connection.brute.Force	41.224.59.166	172.18.48.154	3389	111
Total				**925**

Tabla 4: Eventos inicio de sesión RDP por fuerza bruta mediante solicitudes RDP

3.3. Evento y comportamiento Apache.Strts.2.Jakarta.Multipart.Parser.Code.Exceution

Esto indica un intento de ataque para explotar una vulnerabilidad remota de ejecución de código en Apache Struts. La vulnerabilidad se debe a un problema de manejo de errores cuando la aplicación maneja una solicitud HTTP creada que contiene un campo malicioso de "Tipo de contenido" o "Disposición de contenido". Un atacante remoto puede explotar esto para ejecutar código arbitrario dentro del contexto de la aplicación, a través de una solicitud elaborada.

Ataques	Srcip	Dstip	Dstport	Cantidad Ataques
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execute	185.222.210.57	172.22.156.166	81	221
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execute	185.222.210.57	172.22.156.167	80	110
Total				**331**

Tabla 5: Eventos en Apache Struts

3.4. Evento y comportamiento Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization

Esto indica un intento de ataque contra una vulnerabilidad de ejecución de comandos del sistema operativo en Redhat JBoss Application Server, la vulnerabilidad se debe a un error en la aplicación vulnerable al manejar una solicitud creada de forma malintencionada. Un atacante remoto puede explotar esto para ejecutar código arbitrario dentro del contexto de la aplicación a través de solicitudes elaboradas, para este tipo de vulnerabilidades existen parches que pueden ser descargados del siguiente link https://access.redhat.com/security/cve/cve-2017-12149.

Ataques	Srcip	Dstip	Dstport	Cantidad Ataques
Red.Hat.Jboss.AS.doFilter.Insecure.Deserialization	195.22.127.93	172.22.156.167	80	145
Red.Hat.Jboss.AS.doFilter.Insecure.Deserialization	93.88.74.184	172.22.156.166	81	32
Red.Hat.Jboss.AS.doFilter.Insecure.Deserialization	93.88.74.184	172.22.156.167	80	33
Total				**210**

Tabla 6: Eventos en Redhat JBoss Application Server

3.5. Evento y comportamiento Jboss.JMX.Console.Beanshell.Deployer. War.Upload

Es indica un posible ataque contra un problema de omisión de autenticación en RedHat JBoss Enterprise Application Plataform que podría permitir la carga arbitraria de archivos .war, se conoce que para este tipo de vulnerabilidades afecta los productos RedHat JBoss Enterprose Application Plataform 4.3, 4.3 EL5, 4.3 EL4, 4.2, 4,2 EL5 y 4,2 EL4, se recomienda generalmente mantener el software actualizado, este repositorio de updates se puede concentrar en el siguiente link https://rhn.redhat.com/errata/RHSA-2010-0378.html.

Ataques	Srcip	Dstip	Dstport	Cantidad Ataques
Jboss.JMX.Console.Beanshell.Deployer. War.Upload	185.222.210.57	172.22.156.166	81	125
Jboss.JMX.Console.Beanshell.Deployer. War.Upload	185.222.210.57	172.22.156.167	80	60
Total				**185**

Tabla 7: Eventos en RedHat JBoss Enterprise Application Plataform

4. Análisis intentos de ataques recurrentes por mes

En la verificación de los logs generados por el IPS, se realiza un análisis comparativo por mes en el cual se consolidan los eventos más recurrentes en tal periodo.

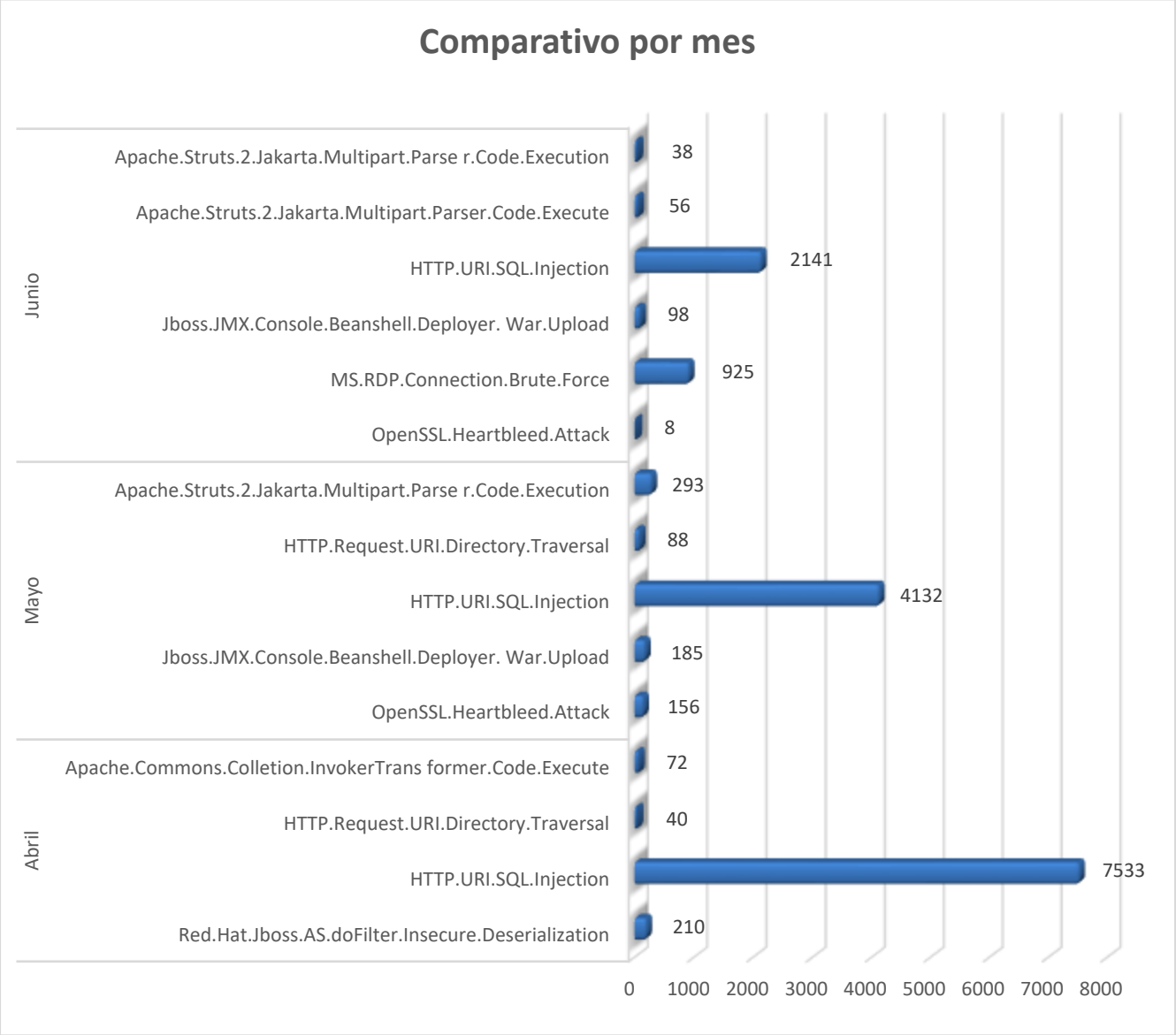


Tabla 8: Intentos de ataques por mes.

B. Depuración de reglas en el firewall

Durante el transcurso de los meses de marzo a septiembre del 2018, y como parte de los objetivos previamente establecidos, se llevó a cabo un Análisis de Seguridad del firewall de Keralty.

Se establece un plan que en cual se contempló los siguientes puntos de análisis:

- ✓ Análisis de las políticas configuradas en firewall de Keralty a fin de evaluar el nivel accesos y permisos que se tienen.
- ✓ Se realiza el análisis del por qué el firewall no tiene licencia y si es necesario adquirirla
- ✓ Se establece la Implementación de formatos para solicitudes de cambios debido a que no se lleva un control en el cual debería quedar registrado los cambios realizados.
- ✓ Asignación de contraseñas seguras para las vpns cliente o remotas, se identificó que las contraseñas que se están asignando por parte del área de nivel uno no son contraseñas fuertes.
- ✓ Generación de reportes de los servicios o los eventos más relevante sobre el tráfico que está pasando por la red de Keralty.

El objeto final de este análisis será el de identificar la existencia de debilidades o vulnerabilidades, e incluso analizar si fuese posible la explotación de las mismas por parte de un atacante midiendo el nivel de intrusión que este último podría obtener. De esta manera se intenta medir el nivel de eficiencia de los controles destinados a asegurar la disponibilidad, la integridad y la confidencialidad de los servicios brindados.

1. Solución Planteada

Durante el desarrollo se realizará la reorganización y el afinamiento de las políticas configuradas en el FIREWALL DE TRIARA que presta el servicio de Tráfico Seguro. Para esta reorganización se utilizará como apoyo varios reportes de tráfico para identificar las aplicaciones y los recursos que están generando mayor consumo de tráfico.

Se realizará además los aseguramientos de las políticas que presentan algún tipo de

vulnerabilidad como es el caso de las políticas que no tienen restricción de servicios, para esto se realizara un análisis de la políticas actualmente configuradas y se realizara un afinamiento de ellas.

2. Revisión de configuración de políticas de Firewall Triara

Al realizar un análisis de las reglas del firewall se puede observar que hay reglas en las cuales tienen habilitados todos los servicios, sin importar hacia donde vaya, a continuación se hace una estadística de las políticas configuradas en el firewall.

ESTADISTICA DE REGLAS CONFIGURADAS	
REGLAS DESHABILITADAS	129
REGLAS SIN TRAFICO	433
REGLAS CON TRAFICO	581
ALL-ALL-ALL	1
XXX-ALL-ALL	47
XXX-XXX-ALL	192
ALL-ALL-XXX	1
ALL-XXX-XXX	52
ALL-XXX-ALL	9
XXX-ALL-XXX	26
TOTAL	1471

Tabla 9: Estadística de reglas configuradas del firewall

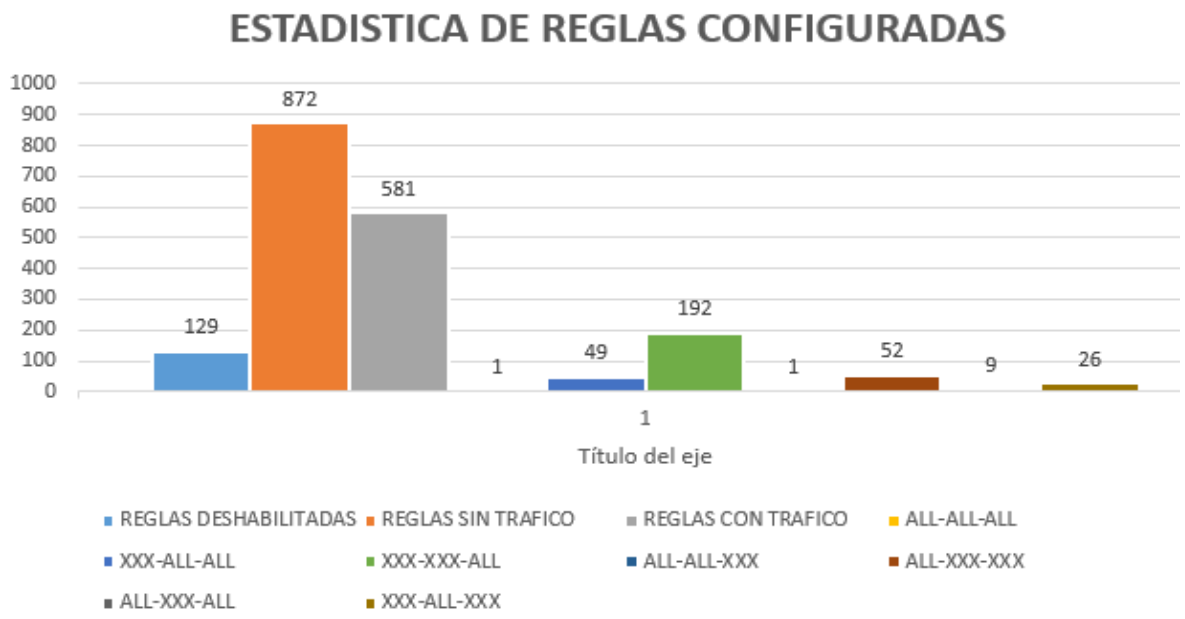


Figura 6: Diagrama de barras de las reglas configuradas

Para cumplir con nuestro objetivo se realizó la depuración de las REGLAS SIN TRAFICO las cuales se deshabilitaron durante un periodo de 2 meses y posteriormente se procede a realizar la eliminación de las estas reglas, estas reglas se eliminaron para evitar que los datos corporativos en cual incluyen información del personal, propiedades intelectuales y datos financieros, nómina, acuerdos del empleado, y cualquier información utilizada para tomar decisiones de empleo sea utilizada de forma inadecuada atreves de las política que se encuentran creadas.

Figura 7: Diagrama de reglas sin tráfico y eliminadas

Se realiza un análisis de tráfico del firewall para restringir los accesos de las políticas Origen XXX- Destino ALL- Servicios ALL, los cuales tienen acceso a diferentes destinos, estas reglas representan un riesgo grande de seguridad para la compañía como se muestra en la figura 8.

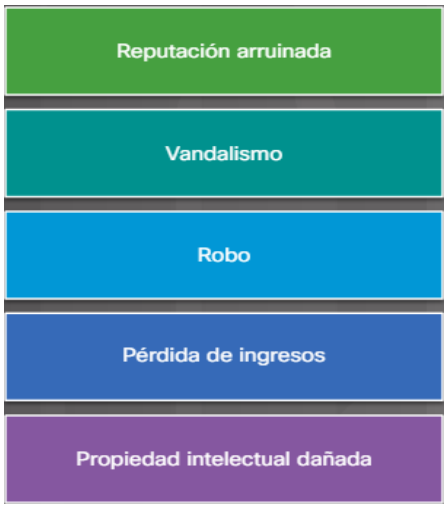


Figura 8: Consecuencias de una violación a la seguridad

Para esto se realizó un análisis de tráfico de 47 reglas en el firewall en cual se puedo identificar cuáles eran sus destinos y los servicios utilizados para cada política el mecanismo utilizado fue el de realizar sniffers sobre cada una de las reglas para establecer dichos destinos y servicios, el resultado de este análisis se puede encontrar en el documento anexo Informe de reglas firewall, se realizó este análisis con el fin de restringir el acceso a Un usuario interno, como un empleado o un partner contratado, puede de manera accidental o intencional realizar las siguientes ataques:

- ✓ Manipular de manera incorrecta los datos confidenciales.
- ✓ Amenazar las operaciones de los servidores internos o de los dispositivos de la infraestructura de red.
- ✓ Facilitar los ataques externos al conectar medios USB infectados al sistema informático corporativo.
- ✓ Invitar accidentalmente al malware a la red con correos electrónicos o páginas web maliciosos.

3. Formatos de Cambios

Se realizó la creación de formatos para solicitudes de cambios en el firewall para llevar control y registro de los cambios realizados en caso de un incidente por una mala configuración o por una mala práctica implementada, estos formatos se encuentran en el anexo Formato_interno_Keralty__de_Gestion_Reglas_firewall, es este formato se estable los datos personales de quien está solicitando la creación o modificación en el firewall, autorización del jefe de área, datos de origen. Destino y servicio, se establece que el formato debe estar completamente diligenciado de lo contrario no se procede a realizar ningún tipo de modificación en el firewall.

Organización Sanitas Internacional

FORMATO DE GESTIÓN DE REGLAS EN FIREWALL

FR-Reglas_FW

16/10/2018

ipo de solicitud:	Creación	OS:	11432239
Fecha Solicitud:	16-oct-18	Ubicación Firewall:	Firewall Triara

Identificación Solicitante

Nombre/Apellidos:	Hamilton Bolaños	Cargo:	Administrador Firewall
Teléfonos:	6466060 Ext. 5711323	e-mail:	hzbolanos@colsanitas.com
Empresa:	Colsanitas / País: Colombia	Ubicación:	calle 100
Tiempo de duración de la regla:	Permanente	Revisión:	***Revisión periodica de reglas funcionales***
Nombre Proyecto:			

Justificación

Buen dia Ingenieros solicito su amable colaboracion para crear las descritas en el formato y entutar las redes 10.247.2540/24 por la red lan port 17 para los biometricos de la empresa Diamante en las diferentes clinicas CUC, CRS, CIB, CSB, CPE a las url y Ip requeridas con sus puertos para lograr conexión exitosa

Impacto en el Negocio	Riesgos del cambio
	Errores humanos en la configuración del Firewall

Autorizaciones

Nombre/Apellidos autorizador Inicial:	Moises Hernandez	Cargo:	Sub Gerente de Tecnologia
Nombres integrantes del comité:		Cargo:	Administrador Firewall
Observaciones del comité:	Aprobado	Fecha revisión comité:	07/07/218

Origen			Puertos			Destino			Puertos			Fechas	
Nombre PC / Red	IP o Rango*	Objet Group	TCP / UDP o Protocolo	Puerto	Objet Group	Nombre o URL destino*	IP o Rango*	Objet Group	Puerto*	TCP / UDP o Protocolo*	Objet Group	Inicio*	Termino*
	[illegible]	[illegible]	[illegible]		[illegible]	http://190.85.45.93/ClienteAdministrativoWeb/AdministratorTerraTestPage.aspx http://sieracrm.sierracloud.com/diamante_crm/index.php?module=Users&action=Login https://drive.google.com/drive/folders/0B0... http://www.brillodoraddiamante.com/procesos/wp-login.php?redirect_to=%2Fprocesos%2F		[illegible]	[illegible]	[illegible]	[illegible]		
	[illegible]	[illegible]			[illegible]	http://190.85.45.93/ClienteAdministrativoWeb/AdministratorTerraTestPage.aspx http://sieracrm.sierracloud.com/diamante_crm/index.php?module=Users&action=Login https://drive.google.com/drive/folders/0B0... http://www.brillodoraddiamante.com/procesos/wp-login.php?redirect_to=%2Fprocesos%2F		[illegible]	[illegible]	[illegible]	[illegible]		

Figura 9: Formato de gestión de reglas en firewall

4. Licenciamiento

Como se observa en la imagen el firewall no contaba con ningún tipo de licenciamiento el cual reduce las capacidades y lo convierte en un firewall tradicional, Al adquirir sin las licencias de antivirus, IPS (Intrusion Prevention System), filtrado de contenido las cuales son de vital importancias para la Organización Keralty ya que con estas aplicaciones se ayuda a detectar patrones basados en ataques y realizar las acciones oportunas de
Bloqueo.

Antes

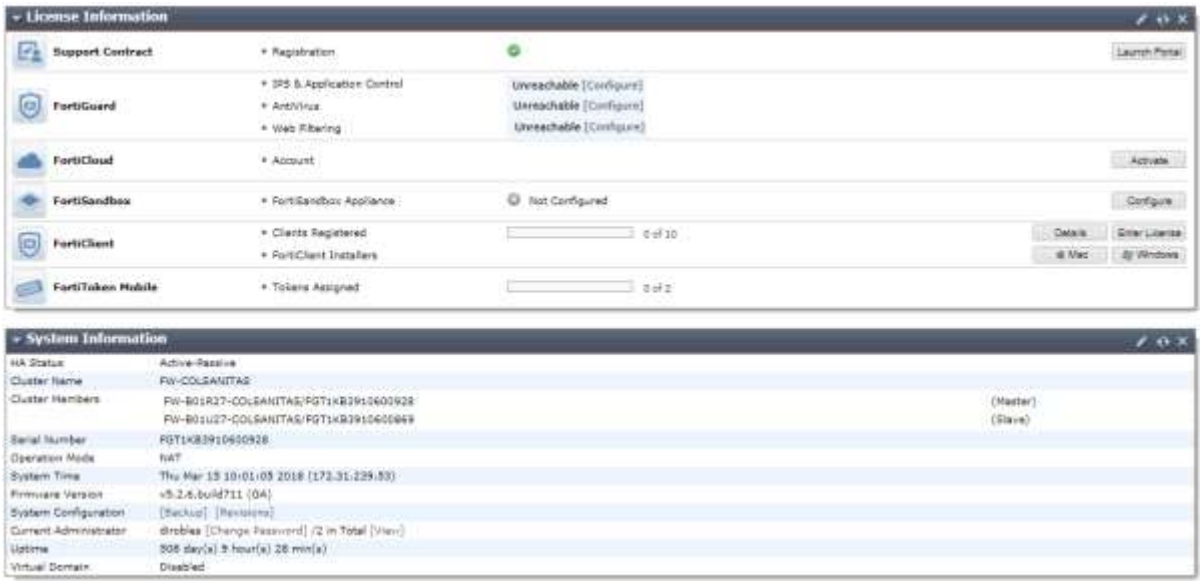


Figura 10: Firewall sin licenciamiento

Ahora

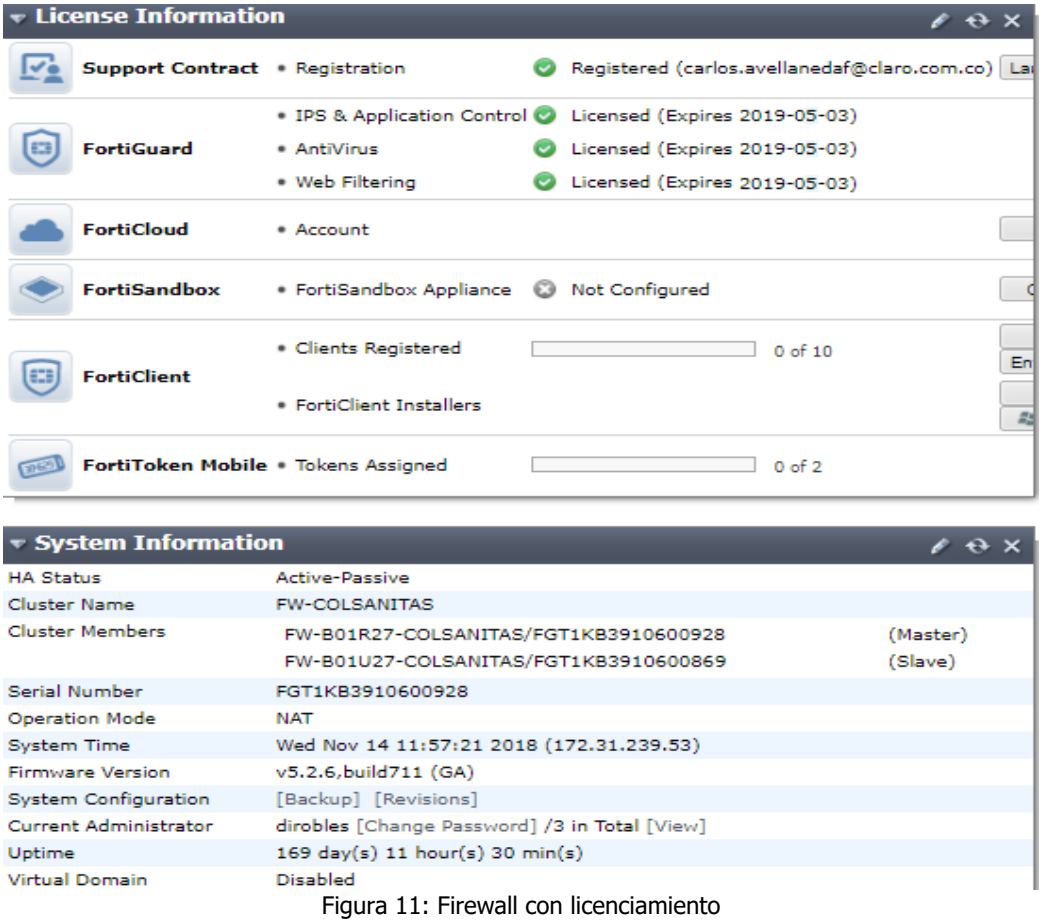


Figura 11: Firewall con licenciamiento

10.4.2. Servidores de preproducción

A. Resultados de las pruebas de vulnerabilidades a los servidores

Para realizar el informe de resultados, que fueron obtenidos luego de la ejecución de la herramienta NESSUS sobre los servidores de preproducción de Keralty, se procede con la documentación de cada vulnerabilidad encontrada para cada dispositivo, además de las recomendaciones de seguridad. Es importante mencionar que en este informe nos centraremos en las vulnerabilidades identificadas en los equipos de la compañía que tengan vulnerabilidades con niveles de severidad CRÍTICA, ALTA Y MEDIA, dejando a un lado las de tipo bajo e informativo.

Para hacer el proceso de análisis de vulnerabilidades se llevó a cabo un proceso metodológico para llevar un seguimiento en el desarrollo del proyecto:

1. Levantamiento de información: Para el levantamiento de información se identificó el rango de direcciones IP objeto de análisis, la cual corresponde a 172.18.46.0. Luego seleccionaremos los servidores con las vulnerabilidades más críticas para realizarles su análisis.
2. Análisis de vulnerabilidades: En la etapa de análisis de vulnerabilidades se utilizaron las herramientas NESSUS y NMAP, las cuales arrojaron 178 IPs correspondientes a los servidores de preproducción, pero solo 14 de ellos serán materia de estudio, teniendo en cuenta que son aquellos que tienen al menos una vulnerabilidad de categoría crítica. Estas herramientas brindaron el estado real de la seguridad de los equipos, adicional, que a partir de este análisis se pueden definir las estrategias para mitigar los riesgos o emprender las acciones de contingencias en los casos de encontrar que los servidores sean susceptibles de ser atacados con impactos relevantes para la empresa.
3. Enunciación de las recomendaciones: Con base a los resultados obtenidos previamente, se procede a proponer las recomendaciones del caso para mitigar los riesgos.

Las vulnerabilidades arrojadas con la herramienta de NESSUS son clasificadas en niveles de severidad o gravedad basada en un puntaje CVSS (métrica estándar de la industria) auto calculado para cada vulnerabilidad especifica de manera numérica de 0.1 – 10.0 y clasificadas en niveles de bajo, medio, alto y crítica. A continuación, se presentan los criterios que definen cada nivel de severidad [11]:

BAJO: Las vulnerabilidades en el rango bajo suelen tener muy poco impacto en el negocio de una organización. La explotación de tales vulnerabilidades generalmente requiere acceso local o físico al sistema.

MEDIO: Las vulnerabilidades que puntúan en el rango medio suelen tener algunas de las siguientes características:

- Las vulnerabilidades que requieren que el atacante manipule a las victimas individuales mediante tácticas de ingeniería social.
- Vulnerabilidades de denegación de servicio que son difíciles de configurar.
- Explotaciones que requieren que un atacante resida en la misma red local que víctima.
- Vulnerabilidades donde la explotación proporciona un acceso muy limitado.
- Vulnerabilidades que requieren privilegios de usuario para una explotación exitosa.

ALTO: Las vulnerabilidades que se puntúan en el rango alto suelen tener algunas de las siguientes características:

- La explotación podría resultar en privilegios elevados.
- La explotación podría resultar en una pérdida significativa de datos o tiempo de inactividad.

CRÍTICA: Las vulnerabilidades que se ubican en este rango generalmente tienen la mayoría de las siguientes características:

- La explotación de la vulnerabilidad probablemente resulte en un compromiso a nivel de raíz de los servidores.
- La explotación suele ser sencilla, en el sentido que el atacante no necesita ninguna credencial de autenticación especial o conocimiento sobre victimas individuales, y no necesita persuadir a un usuario objetivo.

Para las vulnerabilidades críticas, se recomienda que realice parches o actualizaciones lo antes posible.

De otro lado, con base al escaneo de vulnerabilidades se analizarán los servidores de preproducción que tienen al menos una vulnerabilidad con nivel de severidad critica, las cuales fueron las siguientes IPs, comenzando con los servidores de mayor numero vulnerabilidades críticas encontradas:

- 172.18.46.72
- 172.18.46.103
- 172.18.46.33

- 172.18.46.178
- 172.18.46.97
- 172.18.46.28
- 172.18.46.163
- 172.18.46.126
- 172.18.46.224
- 172.18.46.226
- 172.18.46.229
- 172.18.46.230
- 172.18.46.53
- 172.18.46.190

- **IP = 172.18.46.72**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.72, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 13 vulnerabilidades categoría CRITICA
- 2 vulnerabilidades categoría ALTA
- 3 vulnerabilidades categoría MEDIA
- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (13 categoría critica, 2 categoría alta, 3 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Oracle WebLogic Java Object Deserialization RCE (CVE-2015-4852).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS, debido a las llamadas de deserialización inseguras de objetos Java no autenticados a la biblioteca de colecciones de Apache Commons (ACC). Un atacante remoto no autenticado puede explotar esto para ejecutar código Java arbitrario en el contexto del servidor WebLogic.
Solución: Se debe actualizar a la versión fija relevante a la que se hace referencia en el aviso del proveedor.

- **Vulnerabilidad categoría CRÍTICA #2:** Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU) (CVE-2016-0638).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente de Java Messaging Service en la función ReadExternal (), debido a un saneamiento incorrecto de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de una carga útil del objeto diseñado para omitir la lista negra ClassFilet.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2016.

- **Vulnerabilidad categoría CRÍTICA #3:** Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU) (CVE-2016-3510).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente WLS Core en la función readObject() debido a un saneamiento incorrecto de la entrada proporcionada por el usuario.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2016.

- **Vulnerabilidad categoría CRÍTICA #4:** Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU) (CVE-2016-5535).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a las llamadas de deserialización a la Biblioteca de Carga de Archivos de Apache Commons. No se requiere autenticación para explotar esta vulnerabilidad.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2016.

- **Vulnerabilidad categoría CRÍTICA #5:** Oracle WebLogic Server Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU) (CVE-2017-3248).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización insegura de objetos Java por parte del registro RMI.

La falla especifica dentro de la lista insuficiente de ciertos objetos Java. El problema radica en la

falta de validación correcta de os datos proporcionados por el usuario, lo que puede resultar en la deserializacion de los datos que no son de confianza. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código arbitrario en el contexto del proceso actual.

Solución: Aplique el parche adecuado de acuerdo con la recomendación de actualización de parche crítico de enero de 2017.

- **Vulnerabilidad categoría CRÍTICA #6:** Oracle WebLogic WSAT Code Execution (CVE-2017-10271).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el punto final de WSAT debido a la deserialización insegura de objetos Java codificados en XML. Una vulnerabilidad fácilmente explotable que permite a un atacante no autenticado con acceso a la red a través de T3 ponga en peligro el servidor WebLogic de Oracle.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2017.

- **Vulnerabilidad categoría CRÍTICA #7:** Oracle WebLogic Server Deserialization RCE (CVE-2018-2628).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserializacion insegura de objetos java por parte del resgitro RMI. Esta vulnerabilidad puede ser explotada por un atacante con acceso a la red a través del protocolo T3. El protocolo T3 se utiliza para transportar información entre los servidores WebLogic y otros tipos de programas Java. El protocolo T3 de WebLogic se basa en objetos Java serializados para la comunicación, lo que lo hace particularmente vulnerable a esta clase de error. Estas vulnerabilidades surgen cuando un programa intenta usar datos que fueron serializados (convertidos a otro formato para el transporte).

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018. Sin embargo, según Tenable, el parche no tuvo éxito y este problema aún puede ser explotado.

NOTA: De las 13 vulnerabilidades de categoría crítica que arrojo la herramienta NESSUS, las primeras 7 de ellas están descritas anteriormente, las otras 6 se repitieron durante el escaneo, por tanto, no se tomaran en cuenta para este proyecto.

- **Vulnerabilidad categoría ALTA #1**: Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización insegura de los objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Solución: Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.

NOTA: De las 2 vulnerabilidades de categoría alta que arrojo la herramienta NESSUS, la primera de ella esta descrita, la otra vulnerabilidad aparece repetida, por tanto, no se tomara en cuenta para este proyecto.

- **Vulnerabilidad categoría MEDIA#1**: SSH Weak Algorithms Suported

Descripción: Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con las claves débiles.

Solución: Ponerse en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.

- **Vulnerabilidad categoría MEDIA #2:** mDNS Detection (Remote Network)

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Solución: Filtre el trafico entrante al puerto UDP 5353.

- **Vulnerabilidad categoría MEDIA #3:** AMQP Cleartext Authentication

Descripción: El servicio remoto del Protocolo Avanzado de Message Queue Server (AMQP) admite uno o más mecanismos de autenticación que permiten que las credenciales se envíen de forma clara.

Solución: Desactive los mecanismos de autenticación de texto claro en la configuración AMQP.

- **IP = 172.18.46.103**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.103, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 7 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 3 vulnerabilidades categoría MEDIA
- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (7 categoría critica, 1 categoría alta, 3 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Oracle WebLogic Java Objetc Desealization RCE (CVE-2015-4852)

Descripción: Una vulnerabilidad de deserialización que involucra a Apache Commons y Oracle WebLogic Server. Esta es una vulnerabilidad de ejecución remota de código y es explotable de forma remota sin autenticación, es decir, puede explotarse a través de una red sin la necesidad de un nombre de usuario y contraseña.

Solución: Debido a la gravedad de esta vulnerabilidad, Oracle recomienda a los clientes que apliquen las actualizaciones proporcionadas por esta alerta de seguridad tan pronto como sea posible.

- **Vulnerabilidad categoría CRÍTICA #2:** Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU) (CVE-2016-0638).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente de Java Messaging Service en la función ReadExternal (), debido a un saneamiento incorrecto de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede explotar esto, a través de una carga útil del objeto diseñado para omitir la lista negra ClassFilet.class y ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2016.

- **Vulnerabilidad categoría CRÍTICA #3:** Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU) (CVE-2016-3510).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de

ejecución remota de código en el componente WLS Core en la función readObject() debido a un saneamiento incorrecto de la entrada proporcionada por el usuario.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2016.

- **Vulnerabilidad categoría CRÍTICA #4:** Oracle WebLogic Server Java Object Deserialization RCE (Octuber 2016 CPU) (CVE-2016-5535).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a las llamadas de deserialización a la Biblioteca de Carga de Archivos de Apache Commons. No se requiere autenticación para explotar esta vulnerabilidad.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2016.

- **Vulnerabilidad categoría CRÍTICA #5:** Oracle WebLogic Server Java Object Deserialization RCE (January 2017 CPU) (CVE-2017-3248).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización insegura de objetos Java por parte del registro RMI.

La falla especifica dentro de la lista insuficiente de ciertos objetos Java. El problema radica en la falta de validación correcta de os datos proporcionados por el usuario, lo que puede resultar en la deserializacion de los datos que no son de confianza. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código arbitrario en el contexto del proceso actual.

Solución: Aplique el parche adecuado de acuerdo con la recomendación de actualización de parche crítico de enero de 2017.

- **Vulnerabilidad categoría CRÍTICA #6:** Oracle WebLogic WSAT Remote Code Execution (CVE-2017-10271).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el punto final de WSAT debido a la deserialización insegura de objetos Java codificados en XML.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2017.

- **Vulnerabilidad categoría CRÍTICA #7:** Oracle WebLogic Server Deserialization RCE (CVE-2018-2628).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserializacion insegura de objetos java por parte del resgitro RMI. Esta vulnerabilidad puede ser explotada por un atacante con acceso a la red a través del protocolo T3. El protocolo T3 se utiliza para transportar información entre los servidores WebLogic y otros tipos de programas Java. El protocolo T3 de WebLogic se basa en objetos Java serializados para la comunicación, lo que lo hace particularmente vulnerable a esta clase de error. Estas vulnerabilidades surgen cuando un programa intenta usar datos que fueron serializados (convertidos a otro formato para el transporte).

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018. Sin embargo, según Tenable, el parche no tuvo éxito y este problema aún puede ser explotado.

- **Vulnerabilidad categoría ALTA #1**: Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización insegura de los objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Solución: Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.

- **Vulnerabilidad categoría MEDIA #1**: SSH Weak Algorithms Suported

Descripción: Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con las claves débiles.

Solución: Ponerse en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.

- **Vulnerabilidad categoría MEDIA #2:** mDNS Detection (Remote Network)

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como

ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Solución: Filtre el trafico entrante al puerto UDP 5353.

- **Vulnerabilidad categoría MEDIA #3:** AMQP Cleartext Authentication

Descripción: El servicio remoto del Protocolo Avanzado de Message Queue Server (AMQP) admite uno o más mecanismos de autenticación que permiten que las credenciales se envíen de forma clara.

Solución: Desactive los mecanismos de autenticación de texto claro en la configuración AMQP.

- **IP = 172.18.46.33**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.33, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 4 vulnerabilidades categoría CRITICA
- 2 vulnerabilidades categoría ALTA
- 0 vulnerabilidades categoría MEDIA
- 1 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (4 categoría critica, 2 categoría alta, 0 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Oracle WebLogic Server Java Object Deserialization RCE (Octuber 2016 CPU) (CVE-2016-5535).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el componente de seguridad WLS debido a las llamadas de deserialización a la Biblioteca de Carga de Archivos de Apache Commons. No se requiere autenticación para explotar esta vulnerabilidad.

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2016.

- **Vulnerabilidad categoría CRÍTICA #2:** Oracle WebLogic Server Deserialization RCE (CVE-2018-2628).

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserializacion

insegura de objetos java por parte del resgitro RMI. Esta vulnerabilidad puede ser explotada por un atacante con acceso a la red a través del protocolo T3. El protocolo T3 se utiliza para transportar información entre los servidores WebLogic y otros tipos de programas Java. El protocolo T3 de WebLogic se basa en objetos Java serializados para la comunicación, lo que lo hace particularmente vulnerable a esta clase de error. Estas vulnerabilidades surgen cuando un programa intenta usar datos que fueron serializados (convertidos a otro formato para el transporte).

Solución: Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018. Sin embargo, según Tenable, el parche no tuvo éxito y este problema aún puede ser explotado.

NOTA: De las 4 vulnerabilidades de categoría crítica que arrojo la herramienta NESSUS, las primeras 2 de ellas están descritas anteriormente, las otras 2 se repitieron durante el escaneo, por tanto, no se tomaran en cuenta para este proyecto.

- **Vulnerabilidad categoría ALTA #1**: Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Descripción: El servidor remoto de Oracle WebLogic se ve afectado por una vulnerabilidad de ejecución remota de código en el subcomponente Core Components debido a la deserialización insegura de los objetos Java. Un atacante remoto no autenticado puede explotar esto, a través de un objeto Java diseñado, para ejecutar código Java arbitrario en el contexto del servidor WebLogic.

Solución: Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.

NOTA: De las 2 vulnerabilidades de categoría alta que arrojo la herramienta NESSUS, la primera de ellas esta descrita anteriormente, la otra vulnerabilidad se repitió durante el escaneo, por tanto, no se tomara en cuenta para este proyecto.

- **IP 172.18.46.178**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.178, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 3 vulnerabilidades categoría CRITICA
- 13 vulnerabilidades categoría ALTA
- 29 vulnerabilidades categoría MEDIA

- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (3 categoría critica, 13 categoría alta, 29 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Apache 2.2.x <2.2.15 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de Apache 2.2.x que se ejecuta en el host remoto es anterior a la 2.2.15. Por lo tanto, es potencialmente afectado por múltiples vulnerabilidades:

- Es posible un ataque de inyección de prefijo de renegociación TLS (CVE-2009-3555).
- El módulo 'mod_proxy_ajp' devuelve el código de estado incorrecto si encuentra un error que hace que el servidor de servicios de fondo se ponga en un estado de error (CVE-2010-0408).
- El 'mod_isapi' intenta descargar el 'ISAPI.dll' cuando encuentra varios estados de error que podrían dejar las devoluciones de llamada en un estado indefinido (CVE-2010-0425).
- Una falla en el código del proceso de sub-solicitud principal puede llevar a que la información confidencial de una solicitud sea manejada por un subproceso incorrecto si se usa un entorno de subprocesos múltiples (CVE-2010-0434).
- Se agregó el módulo 'mod_reqtimeout' para mitigar los ataques de Slowloris (CVE-2007-6750).

Solución: Actualiza a la versión 2.2.15 de Apache o posterior

- **Vulnerabilidad categoría CRÍTICA #2:** Apache 2.2.x <2.2.13 APR apr_palloc Heap Overflow (CVE-2009-2412).

Descripción: Según su banner autoinformado, la versión de Apache 2.2.x que se ejecuta en el host remoto es anterior a la 2.2.13. Como tal, incluye una versión empaquetada de la biblioteca Apache Portable Runtime (APR) que contiene una falla en 'apr_palloc ()' que podría causar un desbordamiento de pila.

Tenga en cuenta que el servidor HTTP Apache en sí mismo no le pasa a esta función el tamaño no saneado ni provisto por el usuario, por lo que solo podría activarse a través de alguna otra aplicación que lo use de forma vulnerable.

Solución: Actualizar a Apache 2.2.13 o posterior.

- **Vulnerabilidad categoría CRÍTICA #3:** PHP Unsupported Version Detection.

Descripción: Según su versión, la instalación de PHP en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualiza a una versión de PHP que actualmente es compatible.

- **Vulnerabilidad categoría ALTA #1**: PHP <5.2.6 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de PHP instalada en el host remoto es más antigua que 5.2.6. Dichas versiones pueden verse afectadas por los siguientes problemas (CVE-2007-4850, CVE-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051):

- Un desbordamiento de búfer basado en pila en FastCGI SAPI.
- Un desbordamiento de entero en printf ().
- Un problema de seguridad derivado de un cálculo incorrecto de la longitud de PATH_TRANSLATED en cgi_main.c.
- Un bypass safe_mode en cURL.
- Manejo incompleto de caracteres multibyte dentro de escapeshellcmd ().
- Problemas en la PCRE incluida solucionada por la versión 7.6.

Solución: Actualizar a la versión de PHP 5.2.6 o posterior.

- **Vulnerabilidad categoría ALTA #2:** Unsupported Web Server Detection

Descripción: Según su versión, el servidor web remoto está obsoleto y ya no es mantenido por su proveedor o proveedor.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

Solución: Eliminar el servicio si ya no es necesario. De lo contrario, actualice a una versión más nueva si es posible o cambie a otro servidor.

- **Vulnerabilidad categoría ALTA #3:** PHP 5 <5.2.7 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de PHP instalada en el host remoto es anterior a 5.2.7. Por lo tanto, está afectado por múltiples vulnerabilidades:

- Hay un defecto de desbordamiento de búfer en la biblioteca PCRE incluida que permite un ataque de denegación de servicio. Existen múltiples vulnerabilidades de directorio en funciones como 'posix_access', 'chdir' y 'ftok' (CVE-2008-2371).
- Existen múltiples vulnerabilidades de directorio en funciones como 'posix_access', 'chdir' y 'ftok' que permiten que un atacante remoto omita 'safe_mode' (CVE-2008-2665, CVE-2008-2666).

- Se puede desencadenar una falla de desbordamiento de búfer en 'php_imap.c' cuando se procesan encabezados de mensajes largos debido al uso de llamadas de API obsoletas. Esto puede ser explotado para causar una denegación de servicio o para ejecutar código arbitrario (CVE-2008-2829).
- Un desbordamiento de búfer en la función 'imageloadfont' en 'ext / gd / gd.c' puede activarse cuando se proporciona una fuente especialmente diseñada. Esto puede ser explotado para causar una denegación de servicio o para ejecutar código arbitrario (CVE-2008-3658).
- Existe un defecto de desbordamiento de búfer en la función interna 'memnstr' de PHP que puede ser explotada por un atacante utilizando el argumento delimitador para la función 'explotar'. Esto se puede usar para provocar una denegación de servicio o para ejecutar código arbitrario (CVE-2008-3659).
- Cuando PHP se usa como un módulo FastCGI, un atacante que solicita un archivo cuya extensión de nombre de archivo está precedida por varios puntos puede causar una denegación de servicio (CVE-2008-3660).
- Un error de desbordamiento de búfer basado en el montón en la extensión mbstring se puede activar a través de una cadena especialmente diseñada que contiene una entidad HTML que no se maneja durante la conversión de Unicode. Esto se puede explotar para ejecutar código arbitrario (CVE-2008-5557).
- La inicialización incorrecta de las variables globales 'page_uid' y 'page_gid' cuando PHP se usa como un módulo de Apache permite eludir la restricción de seguridad debido a la función SAPI 'php_getuid' sobrecarga (CVE-2008-5624).
- PHP no impone las restricciones correctas cuando 'safe_mode' está habilitado a través de una configuración 'php_admin_flag' en 'httpd.conf'. Esto permite a un atacante, colocando una entrada 'php_value' especialmente diseñada en '.htaccess' (CVE-2008-5625).
- La función 'ZipArchive :: extractTo' en la extensión ZipArchive no puede filtrar secuencias transversales de directorios de nombres de archivos. Un atacante puede explotar esto para escribir en archivos arbitrarios (CVE-2008-5658).
- En circunstancias limitadas, un atacante puede provocar que se produzca un truncamiento de archivo al llamar a la función 'dba_replace' con un argumento no válido (CVE-2008-7068).

- Existe un error de desbordamiento de búfer en la función 'date_from_ISO8601' dentro del archivo 'xmlrpc.c' porque la entrada proporcionada por el usuario no está validada correctamente. Esto puede ser explotado por un atacante remoto para provocar una denegación de servicio o para ejecutar código arbitrario (CVE-2014-8626).

Solución: Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución debido a una regresión en esa versión que hace que la configuración 'magic_quotes_gpc' permanezca desactivada, incluso si estaba activada.

- **Vulnerabilidad categoría ALTA #4:** PHP <5.2.8 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de PHP instalada en el host remoto es anterior a 5.2.8. Como tal, puede verse afectado por las siguientes vulnerabilidades:

- PHP no puede desinfectar correctamente los mensajes de error de HTML o código de script arbitrario, permitiría el código para ataques de scripts entre sitios si la configuración 'display_errors' de PHP está habilitada (CVE-2008-5814).
- La versión 5.2.7 introdujo una regresión con respecto a la funcionalidad 'magic_quotes' debido a una corrección incorrecta de la extensión del filtro. Como resultado, la configuración 'magic_quotes_gpc' permanece desactivada incluso si está activada (CVE-2008-5844).

Solución: Actualiza a la versión 5.2.8 de PHP o posterior.

- **Vulnerabilidad categoría ALTA #5:** PHP <5.2.11 Multiple Vulenerabilities (CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, CVE-2009-5016).

Descripción: Según su banner, la versión de PHP instalada en el host remoto es anterior a 5.2.11. Dichas versiones pueden verse afectadas por varios problemas de seguridad:

- Se produce un error no especificado en la validación de certificado dentro de 'php_openssl_apply_verification_policy'.
- Una vulnerabilidad de validación de entrada no especificada afecta el índice de color en 'imagecolortransparent ()'.
- Una vulnerabilidad de validación de entrada no especificada afecta el procesamiento exif.
- Llamar a 'popen ()' con un modo no válido puede causar un bloqueo en Windows. (Error # 44683).

- Un desbordamiento de enteros en 'xml_utf8_decode ()' puede hacer que sea más fácil eludir los mecanismos de protección de inyección de secuencias de comandos entre sitios y SQL utilizando una cadena especialmente diseñada con una codificación UTF-8 larga. (Bug # 49687).
- 'proc_open ()' puede omitir 'safe_mode_protected_env_vars'. (Bug # 49026).

Solución: Actualiza a la versión de PHP 5.2.11 o posterior.

- **Vulnerabilidad categoría ALTA #6:** PHP 5.2 <5.2.14 Multiple Vulnerabilities.

Descripción: De acuerdo con su banner, la versión de PHP 5.2 instalada en el host remoto es anterior a 5.2.14. Dichas versiones pueden verse afectadas por varios problemas de seguridad:

- Existe un error al procesar solicitudes XML-RPC no válidas que pueden llevar a una falta de referencia del puntero NULO. (error # 51288).
- Existe un error en la función 'fnmatch' que puede provocar el agotamiento de la pila.
- Existe un error en la extensión sqlite que podría permitir el acceso arbitrario a la memoria.
- Existe un error de corrupción de memoria en la función 'substr_replace'.
- Las siguientes funciones no están protegidas adecuadamente contra las interrupciones de funciones: addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, strstr, str_pad, str_word_count, ajuste de línea, strtok, setcookie, strip_tags, molduras, ltrim, rtrim, parse_str, paquete, desempaquetar, uasort, preg_match, strrchr, strchr, substr, str_repeat (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010- 2190, CVE-2010-2191, CVE-2010-2484).
- Los siguientes códigos de operación no están protegidos adecuadamente contra las interrupciones de la función: ZEND_CONCAT, ZEND_ASSIGN_CONCAT, ZEND_FETCH_RW (CVE-2010-2191)
- El serializador de sesión predeterminado contiene un error que se puede explotar al asignar variables de sesión con nombres definidos por el usuario. Los valores serializados arbitrarios se pueden inyectar en las sesiones al incluir el carácter PS_UNDEF_MARKER, '!' En los nombres de las variables.
- Existe un error de uso después de la liberación en la función spl_object_storage_attach'.

- Existe una vulnerabilidad de divulgación de información en la función 'var_export' cuando se manejan ciertas condiciones de error.

Solución: Actualizar a la versión 5.2.14 de PHP o posterior.

- **Vulnerabilidad categoría ALTA #7:** PHP <5.3.9 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de PHP instalada en el host remoto es más antigua que 5.3.9. Como tal, puede verse afectado por los siguientes problemas de seguridad:

- La función 'is_a ()' en PHP 5.3.7 y 5.3.8 desencadena una llamada a '__autoload ()' (CVE-2011-3379).
- Es posible crear una condición de denegación de servicio al enviar múltiples solicitudes especialmente diseñadas que contienen valores de parámetros que causan colisiones de hash cuando se calculan los valores de hash para el almacenamiento en una tabla hash (CVE-2011-4885).
- Existe un desbordamiento de entero en la función exif_process_IFD_TAG en exif.c que puede permitir a un atacante remoto leer ubicaciones de memoria arbitrarias o causar una condición de denegación de servicio. Esta vulnerabilidad solo afecta a PHP 5.4.0beta2 en plataformas de 32 bits (CVE-2011-4566).
- Las llamadas a libxslt no están restringidas a través de xsltSetSecurityPrefs (), lo que podría permitir que un atacante cree o sobrescriba archivos, lo que resulta en la ejecución de código arbitrario (CVE-2012-0057).
- Existe un error en la función 'tidy_diagnose' que puede permitir que un atacante provoque que la aplicación elimine la referencia a un puntero NULL. Esto hace que la aplicación se bloquee (CVE-2012-0781).
- La implementación 'PDORow' contiene un error que puede causar bloqueos en la aplicación al interactuar con la función de sesión (CVE-2012-0788).
- Existe un error en el manejo de la zona horaria, de modo que las llamadas repetidas a la función 'strtotime' pueden permitir un ataque de denegación de servicio a través del consumo de memoria (CVE-2012-0789).

Solución: Actualizar a la versión de PHP 5.3.9 o posterior.

- **Vulnerabilidad categoría ALTA #8:** PHP <5.3.11 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de PHP instalada en el host remoto es anterior a 5.3.11 y, como tal, puede verse afectada por múltiples vulnerabilidades:

- Durante la importación de variables de entorno, los cambios temporales a la directiva 'magic_quotes_gpc' no se manejan correctamente. Esto puede reducir la dificultad de los ataques de inyección de SQL (CVE-2012-0831).
- La variable '$ _FILES' puede estar dañada porque los nombres de los archivos cargados no están validados correctamente (CVE-2012-1172).
- La directiva 'open_basedir' no se maneja adecuadamente con las funciones 'readline_write_history' y 'readline_read_history'.
- La función 'header ()' no detecta los encabezados multilínea con un CR. (Bug # 60227 / CVE-2011-1398).

Solución: Actualizar a la versión de PHP 5.3.11 o posterior.

- **Vulnerabilidad categoría ALTA #9:** PHP <5.3.12 / 5.4.2 CGI Query String Code Execute (CVE-2012-1823).

Descripción: Según su anuncio, la versión de PHP instalada en el host remoto es anterior a la 5.3.12 / 5.4.2, y como tal está potencialmente afectada por una ejecución remota de código y una vulnerabilidad de divulgación de información.
Un error en el archivo 'sapi / cgi / cgi_main.c' puede permitir que un atacante remoto obtenga el código fuente de PHP del servidor web o que pueda ejecutar código arbitrario. En configuraciones vulnerables, PHP trata ciertos parámetros de cadenas de consulta como argumentos de línea de comando, incluidos los interruptores como '-s', '-d' y '-c'. Tenga en cuenta que esta vulnerabilidad solo se puede explotar cuando se utiliza PHP en configuraciones basadas en CGI. Apache con 'mod_php' no es una configuración explotable.
Solución: Actualice a la versión de PHP 5.3.12 / 5.4.2 o posterior. Una solución alternativa 'mod_rewrite' también está disponible.

- **Vulnerabilidad categoría ALTA #10:** Apache 2.2.x <2.2.28 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de Apache 2.2.x que se ejecuta en el host remoto es anterior a 2.2.28. Por lo tanto, está afectado por las siguientes vulnerabilidades:

- Existe una falla dentro del módulo 'mod_headers' que permite a un atacante remoto inyectar encabezados arbitrarios. Esto se hace colocando un encabezado en la parte final de los datos que se envían utilizando la codificación de transferencia fragmentada (CVE-2013-5704).

- Existe una falla dentro del módulo 'mod_deflate' cuando se manejan cuerpos altamente comprimidos. Al usar una solicitud especialmente diseñada, un atacante remoto puede explotar esto para provocar una denegación de servicio agotando los recursos de memoria y CPU (CVE-2014-0118).
- El módulo 'mod_status' contiene una condición de carrera que puede activarse cuando se maneja el marcador. Un atacante remoto puede explotar esto para provocar una denegación de servicio, ejecutar código arbitrario u obtener información confidencial de credenciales (CVE-2014-0226).
- El módulo 'mod_cgid' carece de un mecanismo de tiempo de espera. Al usar una solicitud especialmente diseñada, un atacante remoto puede usar esta falla para provocar una denegación de servicio al hacer que los procesos secundarios se prolonguen indefinidamente, hasta que finalmente se complete el cuadro de indicadores (CVE-2014-0231).

Tenga en cuenta que Nessus no ha evaluado estos problemas, sino que se ha basado únicamente en el número de versión auto informado de la aplicación.

Solución: Actualiza a la versión 2.2.29 de Apache o posterior. Tenga en cuenta que la versión 2.2.28 nunca fue lanzada oficialmente.

- **Vulnerabilidad categoría ALTA #11:** Apache 2.2.x <2.2.33-dev / 2.4.x <2.4.26 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de Apache que se ejecuta en el host remoto es 2.2.x antes de 2.2.33-dev o 2.4.x antes de 2.4.26. Por lo tanto, está afectado por las siguientes vulnerabilidades:

- Existe una vulnerabilidad de omisión de autenticación debido a módulos de terceros que utilizan la función ap_get_basic_auth_pw () fuera de la fase de autenticación. Un atacante remoto no autenticado puede explotar esto para evitar los requisitos de autenticación (CVE-2017-3167).
- Existe un error de desreferencia de puntero NULL debido a llamadas de módulos de terceros a la función mod_ssl ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS. Un atacante remoto no autenticado puede explotar esto para provocar una condición de denegación de servicio (CVE-2017-3169).
- Existe un error de desreferencia de puntero NULL en mod_http2 que se activa cuando se maneja una solicitud HTTP / 2 especialmente diseñada. Un atacante remoto no

autenticado puede explotar esto para provocar una condición de denegación de servicio. Tenga en cuenta que esta vulnerabilidad no afecta a 2.2.x (CVE-2017-7659).

- Existe un error de lectura fuera de los límites en la función ap_find_token () debido a un manejo incorrecto de las secuencias de encabezado. Un atacante remoto no autenticado puede explotar esto, a través de una secuencia de encabezado especialmente diseñada, para provocar una condición de denegación de servicio (CVE-2017-7668).
- Existe un error de lectura fuera de los límites en mod_mime debido al manejo incorrecto de los encabezados de respuesta de Content-Type. Un atacante remoto no autenticado puede explotar esto, a través de un encabezado de respuesta Tipo de Contenido especialmente diseñado, para provocar una condición de denegación de servicio o la divulgación de información confidencial.
  Tenga en cuenta que Nessus no ha evaluado estos problemas, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación (CVE-2017-7679).

Solución: Actualice a Apache versión 2.2.33-dev / 2.4.26 o posterior.

- **Vulnerabilidad categoría ALTA #12:** Apache 2.2.x <2.2.34 Multiple Vulnerabilities.

Descripción: Según su banner, la versión de Apache que se ejecuta en el host remoto es 2.2.x antes de 2.2.34. Por lo tanto, está afectado por las siguientes vulnerabilidades:

- Existe una vulnerabilidad de omisión de autenticación en httpd debido a módulos de terceros que utilizan la función ap_get_basic_auth_pw () fuera de la fase de autenticación. Un atacante remoto no autenticado puede explotar esto para evitar los requisitos de autenticación (CVE-2017-3167).
- Existe una vulnerabilidad de denegación de servicio en httpd debido a una falla de desreferencia de puntero NULL que se activa cuando un módulo de terceros llama a la función mod_ssl ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS. Un atacante remoto no autenticado puede explotar esto para provocar una condición de denegación de servicio (CVE-2017-3169).
- Existe una vulnerabilidad de denegación de servicio en httpd debido a un error de lectura fuera de los límites en la función ap_find_token () que se activa cuando se maneja una secuencia de encabezado de solicitud especialmente diseñada. Un atacante remoto no autenticado puede explotar esto para bloquear el servicio o forzar a ap_find_token () para devolver un valor incorrecto (CVE-2017-7668).

- Existe una vulnerabilidad de denegación de servicio en httpd debido a un error de lectura fuera del límite en el mod_mime que se activa cuando se maneja un encabezado de respuesta Content-Type especialmente diseñado. Un atacante remoto no autenticado puede explotar esto para revelar información confidencial o provocar una condición de denegación de servicio (CVE-2017-7679).
- Existe una vulnerabilidad de denegación de servicio en httpd debido a un error al inicializar o restablecer el marcador de posición de valor en [Proxy-] Encabezados de autorización de tipo 'Digest' antes o entre asignaciones de valor = claves sucesivas por mod_auth_digest. Un atacante remoto no autenticado puede explotar esto, al proporcionar una clave inicial sin asignación '=', para revelar información confidencial o provocar una condición de denegación de servicio (CVE-2017-9788).

Tenga en cuenta que Nessus no ha evaluado estos problemas, sino que solo se ha basado en el número de versión auto informado de la aplicación

Solución: Actualiza a la versión 2.2.34 de Apache o posterior.

- **Vulnerabilidad categoría ALTA #13:** Apache 2.2.x <2.2.14 Multiple Vulnerabilities.

Descripción

Según su banner, la versión de Apache 2.2.x que se ejecuta en el host remoto es anterior a 2.2.14. Por lo tanto, es potencialmente afectado por múltiples vulnerabilidades:

- El manejo de errores defectuoso en el soporte de Solaris pollset podría llevar a una denegación de servicio (CVE-2009-2699).
- El módulo 'mod_proxy_ftp' permite a los atacantes remotos eludir las restricciones de acceso previstas (CVE-2009-3095).
- La función 'ap_proxy_ftp_handler' en 'modules / proxy / proxy_ftp.c' en el módulo 'mod_proxy_ftp' permite que los servidores FTP remotos provoquen una denegación de servicio. Tenga en cuenta que el servidor web remoto puede no verse realmente afectado por estas vulnerabilidades, ya que Nessus no intentó determinar si los módulos afectados están en uso o verificar los problemas en sí mismos (CVE-3094).

Solución: Actualiza a la versión 2.2.14 de Apache o posterior. Alternativamente, asegúrese de que los módulos afectados no estén en uso.

- **Vulnerabilidades categoría MEDIA:** HTTP TRACE / TRACK Methods Allowed, Apache HTTP Server 403 Error Page UTP-7 Encoded XSS, PHP <5.2.4 Multiple Vulnerabilities,

Apache 2.2.x <2.2.6 Multiple Vulnerabilities (DoS, XSS, Disco de información), PHP <5.2.5 Multiple Vulnerabilities, Apache 2.2.x <2.2.8 Multiple Vulnerabilities (XSS, DoS), Apache 2.2.x <2.2.9 Multiple Vulnerabilities (DoS, XSS), PHP <5.2.9 Multiple Vulnerabilities, PHP <5.2.10 Multiple Vulnerabilities, Apache 2.2.x <2.2.12 Multiple Vulnerabilities, PHP <5.2.12 Multiple Vulnerabilities, PHP <5.3.2 / 5.2.13 Multiple Vulnerabilities, Apache 2.2.x <2.2.16 Multiple Vulnerabilities, Apache 2.2.x <2.2.17 Multiple Vulnerabilities, PHP 5.2 <5.2.15 Multiple Vulnerabilities, PHP 5.2 <5.2.17 / 5.3 <5.3.5 Cadena a doble DoS de conversión, Apache 2.2.x <2.2.18 APR apr_fnmatch DoS, Apache 2.2.x <2.2.21 mod_proxy_ajp DoS, Apache 2.2.x <2.2.22 Multiple Vulnerabilities, Apache 2.2.x <2.2.23 Multiple Vulnerabilities, Apache 2.2.x <2.2.24 Multiple Vulnerabilities de XSS, Apache 2.2.x <2.2.25 Multiple Vulnerabilities, PHP PHP_RSHUTDOWN_FUNCTION Security Bypass, Apache 2.2.x <2.2.27 Multiple Vulnerabilities, SMB Signing not required, SSL Medium Strength Cipher Suites Supported, SSL Certificate Wrong Hostname, SSL Certificate Cannont Be Trusted, SSL Self-Signed Certificate.

NOTA: Este servidor tiene 29 vulnerabilidades categoría media, por tanto, para abreviar y no extendernos describiendo cada una de estas vulnerabilidades, solo se nombraron. Para conocerlas en detalle se podrían consultar en el documento anexo a este proyecto.

- **IP = 172.18.46.97**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.97, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 4 vulnerabilidades categoría ALTA
- 15 vulnerabilidades categoría MEDIA
- 4 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 4 categoría alta, 15 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities.

Descripción: Los usuarios no autenticados pueden acceder a los servlets 'EJBInvokerServlet' y 'JMXInvokerServlet' alojados en el servidor web en el host remoto. El host remoto está, por lo

tanto, afectado por las siguientes vulnerabilidades:

- Existe una vulnerabilidad de omisión de seguridad debido a una restricción incorrecta del acceso a las interfaces de administración de la consola y la web. Un atacante remoto no autenticado puede explotar esto, a través de solicitudes directas, para evitar la autenticación y obtener acceso administrativo (CVE-2007-1036).
- Existe una vulnerabilidad de ejecución remota de código debido a que los servlets de invocador JMXInvokerHAServlet y EJBInvokerHAServlet no restringen correctamente el acceso a los perfiles. Un atacante remoto no autenticado puede explotar esto para evitar la autenticación e invocar métodos de MBean, lo que resulta en la ejecución de código arbitrario (CVE-2012-0874).
- Existe una vulnerabilidad de ejecución remota de código en los servlets EJBInvokerServlet y JMXInvokerServlet debido a la capacidad de publicar un objeto acumulado. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud especialmente diseñada, para instalar aplicaciones arbitrarias. Tenga en cuenta que se sabe que este problema afecta a las versiones de McAfee Web Reporter anteriores o iguales a la versión 5.2.1, así como a las versiones de Symantec Workspace Streaming 7.5.0.493 y posiblemente anteriores (CVE-2013-4810).

Solución: Si usa EMC Data Protection Advisor, actualice a la versión 6.x o aplique la solución alternativa a 5.x. o elimine cualquier servlet JBoss afectado.

- **Vulnerabilidad categoría CRÍTICA #2:** JBoss Java Object Deserialization.

Descripción: El servidor remoto de JBoss se ve afectado por varias vulnerabilidades de ejecución remota de código:

- Existe una falla debido a que los servlets de invocadores JMXInvokerHAServlet y EJBInvokerHAServlet no restringen adecuadamente el acceso a los perfiles. Un atacante remoto puede explotar este problema para omitir la autenticación e invocar métodos MBean, permitiendo que se ejecute código arbitrario en el contexto del usuario que ejecuta el servidor (CVE-2012-0874).
- El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código debida a deserialización insegura de objetos Java no autenticados a la biblioteca de colecciones de Apache Commons (ACC). Un atacante remoto no autenticado puede explotar esto, mediante el envío de una solicitud de RMI diseñada para ejecutar código arbitrario en el host de destino (CVE-2015-7501).

Solución: Para la primera vulnerabilidad se recomienda acudir a los avisos del proveedor y alternativamente, asegurarse de que todos los puertos utilizados por el servidor JBoss estén protegidos por el firewall desde cualquier red pública. Con relación a la segunda vulnerabilidad se debe actualizar de acuerdo a lo que ordena Apache commons-collections: Ejecución remota de código durante la deserialización (CVE-2015-7501). Si no se puede arreglar, la manera más rápida de resolver esta vulnerabilidad específica deserialización es eliminar los archivos de clase vulnerables (InvokerTransformer, InstantiateFactory y InstantiateTransformer) en todos los archivos Commons-colecciones tarro. Cualquier cambio manual debe ser probado para evitar complicaciones imprevistas.

Si el paquete de la biblioteca de la colección de recursos comunes en su aplicación, todavía puede ser vulnerable, incluso después de que se apliquen los próximos parches. Tendrá que hacer cambios en la biblioteca de colecciones comunes si empaqueta uno.

- **Vulnerabilidad categoría ALTA #1**: SSL Version 2 and 3 Protocol Detection.

Descripción: El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, que incluyen:

  - Un esquema de relleno inseguro con cifrados CBC.
  - Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de intermediarios o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Si bien SSL / TLS tiene un medio seguro para elegir la versión con mayor compatibilidad del protocolo (de modo que estas versiones solo se utilizarán si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que le permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos estén completamente desactivados.

NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de ejecución encontrada en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía fuerte" del SSC de PCI.

Solución: Deshabilitar SSL 2.0 y 3.0 y en lugar utilizar TLS 1.1 o superior, en conjunto con cifrados aprobados.

- **Vulnerabilidad categoría ALTA #2**: Jboss Enterprise Apllication Platform doFilter() Method Insecure Dererialization RCE (CVE-2017-12149).

Descripción: El servidor de aplicaciones JBoss instalado en el host remoto se ve afectado por una vulnerabilidad de ejecución remota de código. Una falla en el método doFilter de la clase ReadOnlyAccessFilter del servicio HTTP Invoker no restringe las clases para las que realiza la deserialización.

Esto permite que un atacante remoto no autenticado ejecute código arbitrario a través de datos serializados diseñados.

Solución: Asegure el acceso a todos los contextos de http-invoker agregando <url-pattern> / * </url-pattern> a las restricciones de seguridad en el archivo web.xml de http-invoker.sar. Los usuarios que no deseen utilizar el http-invoker.sar pueden eliminarlo.

- **Vulnerabilidad categoría ALTA #3**: JBoss JMX Console Unrestricted Access.

Descripción: El servidor web remoto parece ser una versión de JBoss que permite el acceso no autenticado a los servlets JMX y / o Web Console utilizados para administrar JBoss y sus servicios. Un atacante remoto puede aprovechar este problema para revelar información confidencial sobre la aplicación afectada o incluso tomar el control de ella.

Solución: Asegure o elimine el acceso a JMX y / o la consola web utilizando las opciones de instalación avanzadas.

NOTA: De las 4 vulnerabilidades de categoría alta que arrojo la herramienta NESSUS, 3 de ellas están descritas anteriormente, la otra vulnerabilidad se repitió en el escaneo, por tanto, no se tomara en cuenta para este proyecto.

- **Vulnerabilidad categoría MEDIA #1**: SSH Weak Algorithms Suported

Descripción: Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con las claves débiles.

Solución: Ponerse en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.

- **Vulnerabilidad categoría MEDIA #2**: Apache mod_status /server-status Information Disclosure.

Descripción: Un atacante remoto no autenticado puede obtener una descripción general de la actividad y el rendimiento del servidor web Apache remoto solicitando la URL "/ server-status".

Esta descripción general incluye información como los hosts actuales y las solicitudes que se procesan, el número de trabajadores inactivos y las solicitudes de servicio, y la utilización de la CPU.

Solución: Actualice el (los) archivo (s) de configuración de Apache para desactivar mod_status o restringir el acceso a hosts específicos. También como solución se recomienda configurar la directiva ServerTokens en la configuración de Apache al valor de Prod o ProductOnly; esto le dice a Apache que solo devuelva "Apache" en el encabezado del servidor, devuelto en cada solicitud de página.

- **Vulnerabilidad categoría MEDIA #3**: HTTP TRACE / TRACK Methods Allowed (CVE-2003-1567, CVE-2004-2320, CVE-2010-0386).

Descripción: El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

Un usuario local o remoto sin privilegios puede abusar de la funcionalidad HTTP TRACE para obtener acceso a información confidencial en los encabezados HTTP al realizar solicitudes HTTP a los servidores de la aplicación Sun Java System.

"TRACE" se utiliza simplemente como un mecanismo de eco de datos de entrada para el protocolo HTTP. Este método de solicitud se usa comúnmente para la depuración y otras actividades de análisis de conexión.

La solicitud de rastreo HTTP (que contiene la línea de solicitud, encabezados, datos de publicación), enviada a un rastreo servidor web de soporte, responderá al cliente con la información contenida en la solicitud. TRACE proporciona una manera fácil de saber qué está enviando un cliente HTTP y qué está recibiendo el servidor. Apache, IIS e iPlanet soportan todo el seguimiento tal como lo define el RFC HTTP / 1.1 y actualmente está habilitado de forma predeterminada. Muy pocos administradores de sistemas han deshabilitado este método de solicitud, ya que el método no planteaba un riesgo conocido, las configuraciones predeterminadas se consideraban suficientemente buenas o simplemente no tenían ninguna opción para hacerlo.

Solución: Deshabilitar los métodos HTTP TRACE / TRACK para Sun Java System Application Server 7 y Sun Java System Application Server 7 2004Q2 y luego reinicie el servidor.

- **Vulnerabilidad categoría MEDIA #4**: SSL Certificate Expiry.

Descripción: Este complemento comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha caducado.

Solución: Compre o genere un nuevo certificado SSL para reemplazar el existente.

- **Vulnerabilidad categoría MEDIA #5**: SSL Medium Strength Cipher Suites Supported.

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la fuerza media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.
Tenga en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.
Solución: Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de resistencia media.

- **Vulnerabilidad categoría MEDIA #6:** SSL Certificate Cannot Be Trusted

Descripción: El certificado X.509 del servidor no se puede confiar. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado auto firmado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando la exploración se produce antes de una de las fechas de "no antes" del certificado, o después de una de las fechas de "no después de" del certificado.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas erróneas se pueden arreglar al obtener el certificado con la firma errónea para que el emisor lo vuelva a firmar. Las firmas que no se pudieron verificar son el resultado del emisor del certificado que utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.
Solución: Compre o genere un certificado adecuado para este servicio.

- **Vulnerabilidad categoría MEDIA #7**: SSL Self-Signed Certificate.

Descripción: La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificados reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquier persona podría establecer un ataque de hombre en el medio contra el host remoto.

Solución: Compre o genere un certificado adecuado para este servicio.

- **Vulnerabilidad categoría MEDIA #8:** mDNS Detection (Remote Network)

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Solución: Filtre el trafico entrante al puerto UDP 5353.

- **Vulnerabilidad categoría MEDIA #9:** JBoss Enterprise Application Platform '/web-console' Authentication Bypass (CVE 2010-1428).

Descripción: La versión de JBoss Enterprise Application Platform (EAP) que se ejecuta en el host remoto permite el acceso no autenticado a ciertos documentos en el directorio '/ web-console'. Esto se debe a una mala configuración en 'web.xml' que solo requiere autenticación para las solicitudes GET y POST. Al especificar un comando diferente, como HEAD, DELETE o PUT, se usa el controlador GET predeterminado sin autenticación.

Un atacante remoto puede explotar esto para obtener información confidencial sin proporcionar autenticación.

Es probable que esta versión de JBoss EAP tenga otras vulnerabilidades, aunque Nessus no haya revisado esos problemas.

Solución: Actualice a JBoss EAP versión 4.2.0. CP09 / 4.3.0.CP08 o posterior.

NOTA: De las 15 vulnerabilidades de categoría media que arrojo la herramienta NESSUS, las primeras 9 de ellas están descritas anteriormente, las otras 6 se repitieron durante el escaneo, por tanto, no se tomaran en cuenta para este proyecto.

- **IP = 172.18.46.28**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.28, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 2 vulnerabilidades categoría ALTA
- 2 vulnerabilidades categoría MEDIA
- 1 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 2 categoría alta, 2 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Apache Tomcat/JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities (CVE-2007-1036, CVE-2012-0874, CVE-2013-4810).

Descripción: Los usuarios no autenticados pueden acceder a los servlets 'EJBInvokerServlet' y 'JMXInvokerServlet' alojados en el servidor web en el host remoto. El host remoto está, por lo tanto, afectado por las siguientes vulnerabilidades:
Existe una vulnerabilidad de omisión de seguridad debido a una restricción incorrecta del acceso a las interfaces de administración de la consola y la web. Un atacante remoto no autenticado puede explotar esto, a través de solicitudes directas, para evitar la autenticación y obtener acceso administrativo (CVE-2007-1036).
Existe una vulnerabilidad de ejecución remota de código debido a que los servlets de invocador JMXInvokerHAServlet y EJBInvokerHAServlet no restringen correctamente el acceso a los perfiles (CVE-2012-0874).
Los servlets en JBoss Enterprise Application Platform (EAP) antes de 5.2.0, Web Platform (EWP) antes de 5.2.0, BRMS Platform antes de 5.3.1, y SOA Platform antes de 5.3.1 no requiere autenticación por defecto en ciertos perfiles, lo que podría permitir a los atacantes remotos invocar métodos MBean y ejecutar código arbitrario a través de vectores no especificados. La vulnerabilidad de ejecución remota de código en los servlets EJBInvokerServlet y JMXInvokerServlet debido a la capacidad de publicar un objeto acumulado. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud especialmente diseñada, para instalar aplicaciones arbitrarias. Tenga en cuenta que se sabe que este problema afecta a las versiones de McAfee Web Reporter anteriores o iguales a la versión 5.2.1, así como a las versiones de Symantec Workspace Streaming 7.5.0.493 y posiblemente anteriores (CVE-2013-4810).
Solución: Se debe actualizar a la actualizar a la versión 6.x o elimine cualquier servlet JBoss afectado.

- **Vulnerabilidad categoría CRÍTICA #2:** JBoss Java Object Deserialization RCE (CVE-2015-7501).

Descripción: El servidor remoto de JBoss se ve afectado por múltiples vulnerabilidades de ejecución remota de código entre la que se destaca los ataques remotos con comandos arbitrarios a través de un objeto Java serializado diseñado, relacionado con la biblioteca de colecciones de Apache

Solución: Alternativamente, asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss estén protegidos por firewall desde cualquier red pública.

- **Vulnerabilidad categoría ALTA #1:** JBoss JMX Console Unrestricted Access (CVE-2007-1036).

Descripción: El servidor web remoto parece ser una versión de JBoss que permite el acceso no autenticado a los servlets JMX y o Web Console utilizados para administrar JBoss y sus servicios. Un atacante remoto puede aprovechar este problema para revelar información confidencial sobre la aplicación afectada o incluso tomar el control de ella.

Solución: Asegure o elimine el acceso a JMX o la consola web utilizando las opciones de instalación avanzadas, el uso de las opciones del instalador avanzado configurará JBoss para permitir solo el acceso administrativo autenticado.

- **Vulnerabilidad categoría ALTA #2:** JBoss Enterprise Application Platform do Filter Method Insecure Deserialization RCE (CVE-2017-12149).

Descripción: El servidor de aplicaciones JBoss instalado en el host remoto se ve afectado por una vulnerabilidad de ejecución remota de código. Una falla en el método doFilter de la clase ReadOnlyAccessFilter, del servicio HTTP Invoker no restringe las clases para las que realiza la deserialización.

Solución: Siga las pautas de mitigación proporcionadas en el aviso de Red Hat, Antes de aplicar esta actualización, haga una copia de seguridad de la instalación de la plataforma de aplicación empresarial de Red Hat JBoss y de las aplicaciones implementadas.

- **Vulnerabilidad categoría MEDIA #1:** JBoss Enterprise Application Platform '/web-console' Authentication Bypass (CVE-2010-1428).

Descripción: La versión de JBoss Enterprise Application Platform (EAP) que se ejecuta en el host remoto permite el acceso no autenticado a ciertos documentos en el directorio '/ web-console'. Esto se debe a una mala configuración en 'web.xml' que solo requiere autenticación para las

solicitudes GET y POST. Al especificar un comando diferente, como HEAD, DELETE o PUT, se usa el controlador GET predeterminado sin autenticación.
Un atacante remoto puede explotar esto para obtener información confidencial sin proporcionar autenticación.
Solución: Actualice a JBoss EAP versión 4.2.0. CP09, 4.3.0.CP08 o posterior.

- **Vulnerabilidad categoría MEDIA #2:** mDNS Detection (Remote Network).

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.
Solución: Filtre el tráfico entrante al puerto UDP 5353, si lo desea.

- **IP = 172.18.46.163**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.163, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 2 vulnerabilidades categoría ALTA
- 4 vulnerabilidades categoría MEDIA
- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 2 categoría alta, 4 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Apache Tomcat/JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities.

Descripción: Los usuarios no autenticados pueden acceder a los servlets 'EBJInvokerServlet' y 'JMXInvokerServlet' alojados en el servidor web en el host remoto. El host remoto está, por lo tanto, afectado por las siguientes vulnerabilidades:
Existe una vulnerabilidad de omisión de seguridad debido a una restricción incorrecta del acceso a las interfaces de administración de la consola y la web. Un atacante remoto no autenticado puede explotar esto, a través de solicitudes directas, para evitar la autenticación y obtener acceso administrativo (CVE-2007-1036).
Existe una vulnerabilidad de ejecución remota de código debido a que los servlets de invocador

JMXInvokerHAServlet y EJBInvokerHAServlet no restringen correctamente el acceso a los perfiles (CVE-2012-0874).

Los servlets en JBoss Enterprise Application Platform (EAP) antes de 5.2.0, Web Platform (EWP) antes de 5.2.0, BRMS Platform antes de 5.3.1, y SOA Platform antes de 5.3.1 no requiere autenticación por defecto en ciertos perfiles, lo que podría permitir a los atacantes remotos invocar métodos MBean y ejecutar código arbitrario a través de vectores no especificados

La vulnerabilidad de ejecución remota de código en los servlets EJBInvokerServlet y JMXInvokerServlet debido a la capacidad de publicar un objeto acumulado. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud especialmente diseñada, para instalar aplicaciones arbitrarias. Tenga en cuenta que se sabe que este problema afecta a las versiones de McAfee Web Reporter anteriores o iguales a la versión 5.2.1, así como a las versiones de Symantec Workspace Streaming 7.5.0.493 y posiblemente anteriores (CVE-2013-4810).

Solución: Se debe actualizar a la actualizar a la versión 6.x o elimine cualquier servlet JBoss afectado.

- **Vulnerabilidad categoría CRÍTICA #2:** JBoss Java Object Deserialization RCE (CVE-2015-7501).

Descripción: El servidor remoto de JBoss se ve afectado por múltiples vulnerabilidades de ejecución remota de código entre la que se destaca los ataques remotos con comandos arbitrarios a través de un objeto Java serializado diseñado, relacionado con la biblioteca de colecciones de Apache

Solución: Alternativamente, asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss estén protegidos por firewall desde cualquier red pública.

- **Vulnerabilidad categoría ALTA #1:** JBoss JMX Console Unrestricted Access (CVE-2007-1036).

Descripción: El servidor web remoto parece ser una versión de JBoss que permite el acceso no autenticado a los servlets JMX y o Web Console utilizados para administrar JBoss y sus servicios. Un atacante remoto puede aprovechar este problema para revelar información confidencial sobre la aplicación afectada o incluso tomar el control de ella.

Solución: Asegure o elimine el acceso a JMX o la consola web utilizando las opciones de instalación avanzadas, el uso de las opciones del instalador avanzado configurará JBoss para permitir solo el acceso administrativo autenticado.

- **Vulnerabilidad categoría ALTA #2:** JBoss Enterprise Application Platform do Filter Method Insecure Deserialization RCE (CVE-2017-12149).

Descripción: El servidor de aplicaciones JBoss instalado en el host remoto se ve afectado por una vulnerabilidad de ejecución remota de código. Una falla en el método doFilter de la clase ReadOnlyAccessFilter, del servicio HTTP Invoker no restringe las clases para las que realiza la deserialización.

Solución: Siga las pautas de mitigación proporcionadas en el aviso de Red Hat, Antes de aplicar esta actualización, haga una copia de seguridad de la instalación de la plataforma de aplicación empresarial de Red Hat JBoss y de las aplicaciones implementadas.

- **Vulnerabilidad categoría MEDIA #1:** JBoss Enterprise Application Platform '/web-console' Authentication Bypass (CVE-2010-1428).

Descripción: La versión de JBoss Enterprise Application Platform (EAP) que se ejecuta en el host remoto permite el acceso no autenticado a ciertos documentos en el directorio '/ web-console'. Esto se debe a una mala configuración en 'web.xml' que solo requiere autenticación para las solicitudes GET y POST. Al especificar un comando diferente, como HEAD, DELETE o PUT, se usa el controlador GET predeterminado sin autenticación.

Un atacante remoto puede explotar esto para obtener información confidencial sin proporcionar autenticación.

Solución: Actualice a JBoss EAP versión 4.2.0. CP09, 4.3.0.CP08 o posterior.

- **Vulnerabilidad categoría MEDIA #2:** AMQP Cleartext Authentication

Descripción: El servicio remoto del Protocolo Avanzado de Message Queue Server (AMQP) admite uno o más mecanismos de autenticación que permiten que las credenciales se envíen de forma clara.

Solución: Desactive los mecanismos de autenticación de texto claro en la configuración AMQP.

- **Vulnerabilidad categoría MEDIA #3:** mDNS Detection (Remote Network)

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Solución: Filtre el tráfico entrante al puerto UDP 5353, si lo desea.

- **Vulnerabilidad categoría MEDIA #4:** SSH Weak Algorithms Supported

Descripción: Se ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con las teclas débiles.

Solución: Desactivar los algoritmos de cifrado débil.

- **IP = 172.18.46.126**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.126, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 5 vulnerabilidades categoría MEDIA
- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 1 categoría alta, 5 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** HP Data Protector Unsupported

Descripción: Según su número de versión auto informado, ya no se admite la instalación de HP Data Protector en el host remoto. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualice a una versión de HP Data Protector que actualmente es compatible.

- **Vulnerabilidad categoría CRÍTICA #2:** HP Data Protector Multiple Vulnerabilities (CVE-2013-2347)

Descripción: La instalación remota de HP Data Protector se ve afectada por múltiples vulnerabilidades que podrían permitir a un atacante remoto obtener privilegios elevados, desencadenar una vulnerabilidad de denegación de servicio o, en el peor de los casos, ejecutar código arbitrario. La vulnerabilidad no especificada en HP Storage Data Protector 6.2X permite a los atacantes remotos ejecutar código arbitrario o provocar una denegación de servicio a través de vectores desconocidos, también conocido como ZDI-CAN-2008.

Solución: Actualice a una versión de HP Data Protector que actualmente es compatible.

- **Vulnerabilidad categoría ALTA #1:** rlogin Service Detection

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable

ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.
Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv..
Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **Vulnerabilidad categoría MEDIA #1:** mDNS Detection (Remote Network)

Descripción: El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.
Solución: Filtre el tráfico entrante al puerto UDP 5353, si lo desea.

- **Vulnerabilidad categoría MEDIA #2:** Samba Badlock Vulnerability (CVE-2016-2118)

Descripción: La versión de Samba, un servidor CIFS / SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock, que existe en el Administrador de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD). Protocolos debido a la negociación incorrecta del nivel de autenticación a través de los canales de llamada a procedimiento remoto (RPC). Un atacante hombre en el medio que es capaz de interceptar el tráfico entre un cliente y un servidor que aloja una base de datos SAM puede aprovechar esta falla para forzar una baja del nivel de autenticación, lo que permite la ejecución de llamadas de red Samba arbitrarias. en el contexto del usuario interceptado, como ver o modificar datos de seguridad confidenciales en la base de datos de Active Directory (AD) o desactivar servicios críticos.
Solución: Actualice a la versión 4.2.11 / 4.3.8 / 4.4.2 de Samba o posterior.

- **Vulnerabilidad categoría MEDIA #3:** SMB Signing not required

Descripción: La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediarios contra el servidor SMB.
Solución: Imponer la firma de mensajes en la configuración del host. En Windows, esto se

encuentra en la configuración de la política 'Servidor de red de Microsoft: firmar comunicaciones digitalmente (siempre)'. En Samba, la configuración se llama 'firma de servidor'. WindowsServers: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters

- **Vulnerabilidad categoría MEDIA #4:** HTTP TRACE / TRACK Methods Allowed

Descripción: La configuración predeterminada de Sun Java System Application Server 7 y 7 2004Q2 permite el método HTTP TRACE, que facilita que los atacantes remotos roben cookies y credenciales de autenticación a través de un ataque de rastreo entre sitios (XST).
Solución: Al seleccionar estos enlaces, saldrá del espacio web NIST. Hemos proporcionado estos enlaces a otros sitios web porque pueden tener información que podría ser de su interés. Desactivar estos métodos.

- **IP = 172.18.46.224**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.224, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 0 vulnerabilidades categoría MEDIA
- 3 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 1 categoría alta, 0 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** X11 Server Unauthenticated Access

Descripción: El servidor X11 remoto acepta conexiones desde cualquier lugar. Un atacante puede conectarse a él para escuchar a escondidas los eventos de teclado y mouse de un usuario en el host remoto. Incluso es posible que un atacante haga una captura de pantalla del host remoto o muestre programas arbitrarios. Un atacante puede explotar esta falla para obtener el nombre de usuario y la contraseña de un usuario en el host remoto.
Solución: Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.

- **Vulnerabilidad categoría CRÍTICA #2:** X Server Unauthenticated Access: Screenshot.

Descripción: El servidor remoto acepta conexiones TCP remotas. Es posible que un atacante capture una captura de pantalla del host remoto.

Solución: Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.

- **Vulnerabilidad categoría ALTA #1:** rlogin Service Detection.

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.
Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv.
Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **IP = 172.18.46.226**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.226, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 0 vulnerabilidades categoría MEDIA
- 3 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 1 categoría alta, 0 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** X11 Server Unauthenticated Access

Descripción: El servidor X11 remoto acepta conexiones desde cualquier lugar. Un atacante puede conectarse a él para escuchar a escondidas los eventos de teclado y mouse de un usuario en el host remoto. Incluso es posible que un atacante capture una captura de pantalla del host remoto o muestre programas arbitrarios. Un atacante puede explotar esta falla para obtener el nombre de usuario y la contraseña de un usuario en el host remoto.
Solución: Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.

- **Vulnerabilidad categoría CRÍTICA #2:** X Server Unauthenticated Access: Screenshot.

Descripción: El servidor remoto acepta conexiones TCP remotas. Es posible que un atacante capture una captura de pantalla del host remoto.
Solución: Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.

- **Vulnerabilidad categoría ALTA #1:** rlogin Service Detection.

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.
Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv.
Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **IP = 172.18.46.229**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.229, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 0 vulnerabilidades categoría MEDIA
- 3 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 1 categoría alta, 0 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** X11 Server Unauthenticated Access.

Descripción: El servidor X11 remoto acepta conexiones desde cualquier lugar. Un atacante puede conectarse a él para escuchar a escondidas los eventos de teclado y mouse de un usuario en el host remoto. Incluso es posible que un atacante capture una captura de pantalla del host remoto o muestre programas arbitrarios. Un atacante puede explotar esta falla para obtener el

nombre de usuario y la contraseña de un usuario en el host remoto.

Solución: Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.

- **Vulnerabilidad categoría CRÍTICA #2:** X Server Unauthenticated Access: Screenshot

Descripción: El servidor remoto acepta conexiones TCP remotas. Es posible que un atacante capture una captura de pantalla del host remoto.

Solución: Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.

- **Vulnerabilidad categoría ALTA #1:** rlogin Service Detection

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.

Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv.

Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **IP = 172.18.46.230**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.230, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 2 vulnerabilidades categoría CRITICA
- 1 vulnerabilidades categoría ALTA
- 0 vulnerabilidades categoría MEDIA
- 3 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (2 categoría critica, 1 categoría alta, 0 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** X11 Server Unauthenticated Access.

Descripción: El servidor X11 remoto acepta conexiones desde cualquier lugar. Un atacante

puede conectarse a él para escuchar a escondidas los eventos de teclado y mouse de un usuario en el host remoto. Incluso es posible que un atacante capture una captura de pantalla del host remoto o muestre programas arbitrarios. Un atacante puede explotar esta falla para obtener el nombre de usuario y la contraseña de un usuario en el host remoto.

Solución: Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.

- **Vulnerabilidad categoría CRÍTICA #2:** X Server Unauthenticated Access: Screenshot.

Descripción: El servidor remoto acepta conexiones TCP remotas. Es posible que un atacante capture una captura de pantalla del host remoto.

Solución: Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.

- **Vulnerabilidad categoría ALTA #1:** rlogin Service Detection.

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.

Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv.

Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **IP = 172.18.46.53**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.53, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 1 vulnerabilidades categoría CRITICA
- 3 vulnerabilidades categoría ALTA
- 11 vulnerabilidades categoría MEDIA
- 3 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis

(1 categoría critica, 3 categoría alta, 11 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** rexecd Service Detection (CVE-1999-0618).

Descripción: El servicio rexecd se está ejecutando en el host remoto. Este servicio está diseñado para permitir a los usuarios de una red ejecutar comandos de forma remota.
Sin embargo, rexecd no proporciona ningún buen medio de autenticación, por lo que un atacante puede abusar de él para analizar un host de terceros.
Solución: Comente la línea 'exec' en /etc/inetd.conf y reinicie el proceso inetd.

- **Vulnerabilidad categoría ALTA #1**: rlogin Service Detection (CVE-1999-0651).

Descripción: El servicio rlogin se está ejecutando en el host remoto. Este servicio es vulnerable ya que los datos se pasan entre el cliente rlogin y el servidor en texto sin cifrar. Un atacante hombre en el medio puede explotar esto para rastrear inicios de sesión y contraseñas. Además, puede permitir inicios de sesión mal autenticados sin contraseñas. Si el host es vulnerable a la adivinación del número de secuencia de TCP (desde cualquier red) o la suplantación de IP (incluido el secuestro de ARP en una red local), entonces es posible evitar la autenticación.
Finalmente, rlogin es una forma fácil de convertir el acceso de escritura de archivos en inicios de sesión completos a través de los archivos .rhosts o rhosts.equiv.
Solución: Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.

- **Vulnerabilidad categoría ALTA #2**: Oracle TNS Listener Remote Poisoning (CVE-2012-1675).

Descripción: La escucha remota de Oracle TNS permite el registro del servicio desde un host remoto. Un atacante puede explotar este problema para desviar datos de un servidor o cliente de base de datos legítimos a un sistema especificado por el atacante.
Los ataques exitosos permitirán al atacante manipular instancias de base de datos, lo que posiblemente facilitará los ataques de intermediarios, secuestro de sesión o denegación de servicio en un servidor de base de datos legítimo.
Solución: Las recomendaciones para protegerse de esta vulnerabilidad se puede encontrar en Oracle Support Note 1340831.1 para implementaciones de la base de datos Oracle que utilizan Oracle Real Application Clusters y en Oracle Support Note 1453883.1 para implementaciones de la base de datos Oracle que no usan RAC.

- **Vulnerabilidad categoría ALTA #3**: SSL Versión 2 and 3 Protocol Detection.

Descripción: El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, que incluyen:

- Un esquema de relleno inseguro con cifrados CBC.
- Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de intermediarios o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Si bien SSL / TLS tiene un medio seguro para elegir la versión con mayor compatibilidad del protocolo (de modo que estas versiones solo se utilizarán si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que le permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos estén completamente desactivados.

NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de ejecución encontrada en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía fuerte" del SSC de PCI.

Solución: Deshabilitar SSL 2.0 y 3.0 y en lugar utilizar TLS 1.1 o superior, en conjunto con cifrados aprobados.

- **Vulnerabilidad categoría MEDIA #1**: SSH Weak Algorithms Supported.

Descripción: Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo de Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con las claves débiles.

Solución: Ponerse en contacto con el proveedor o consulte la documentación del producto para eliminar los cifrados débiles.

- **Vulnerabilidad categoría MEDIA #2**: Unencrypted Telnet Server

Descripción: El host remoto ejecuta un servidor Telnet en un canal no cifrado.

No se recomienda utilizar Telnet a través de un canal no cifrado, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto sin cifrar. Esto permite que un atacante remoto, hombre en el medio, escuche a escondidas en una sesión de Telnet para obtener credenciales u otra información confidencial y para modificar el tráfico intercambiado entre un cliente y un servidor.

Se prefiere SSH a Telnet, ya que protege las credenciales de las escuchas ilegales y puede

canalizar flujos de datos adicionales, como una sesión X11.

Solución: Deshabilite el servicio Telnet y use SSH en su lugar.

- **Vulnerabilidad categoría MEDIA #3**: Multiple Mail Server EXPN/VRFY Information Disclosure.

Descripción: El servidor SMTP remoto responde a los comandos EXPN y / o VRFY.

El comando EXPN se puede usar para encontrar la dirección de entrega de los alias de correo, o incluso el nombre completo de los destinatarios, y el comando VRFY se puede usar para verificar la validez de una cuenta.

Su correo no debe permitir que los usuarios remotos usen ninguno de estos comandos, ya que les da demasiada información.

Solución: Si está utilizando Sendmail, agregue la opción: O PrivacyOptions = goaway en /etc/sendmail.cf.

- **Vulnerabilidad categoría MEDIA #4**: Network Time Protocol (NTP) Mode 6 Scanner.

Descripción: El servidor NTP remoto responde a las consultas del modo 6. Los dispositivos que responden a estas consultas tienen el potencial de ser utilizados en ataques de amplificación NTP. Un atacante remoto no autenticado podría potencialmente explotar esto, a través de una consulta de modo 6 especialmente diseñada, para provocar una condición de denegación de servicio reflejada.

Solución: Restringir las consultas del modo NTP 6.

- **Vulnerabilidad categoría MEDIA #5**: X Display Manager Control Protocol (XDMCP) Detection.

Descripción: El servicio X Display Manager Control Protocol (XDMCP) le permite a un usuario de Unix obtener de forma remota un inicio de sesión gráfico de X11 y, por lo tanto, actuar como un usuario local en el host remoto. Si un atacante puede obtener un nombre de usuario y una contraseña válidos, este servicio podría usarse para obtener un mayor acceso en el host remoto. Un atacante también puede usar este servicio para montar un ataque de diccionario contra el host remoto para intentar iniciar sesión de forma remota.

Tenga en cuenta que XDMCP es vulnerable a los ataques de intermediarios, lo que facilita que los atacantes roben las credenciales de los usuarios legítimos mediante la suplantación del servidor XDMCP. Además de esto, XDMCP no es un protocolo cifrado, que permite a un atacante capturar las pulsaciones de teclado introducidas por el usuario.

Solución: Deshabilite el servicio XDMCP, si no lo usa, y no permita que este servicio se ejecute a través de Internet.

- **Vulnerabilidad categoría MEDIA #6**: SSL Weak Cipher Suites Supported.

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado débil. Esto es considerablemente más fácil de explotar si el atacante está en la misma red física. El software almacena o transmite datos confidenciales utilizando un esquema de encriptación que es teóricamente bueno, pero no es lo suficientemente fuerte para el nivel de protección requerido. Un esquema de encriptación débil puede estar sujeto a ataques de fuerza bruta que tienen una probabilidad razonable de tener éxito utilizando los métodos y recursos de ataque actuales.
Solución: Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados débiles.

- **Vulnerabilidad categoría MEDIA #7**: SSL Certificate Signed Using Weak Hashing Algorithm (CVE-2004-2761).

Descripción: El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Solución: La recomendación es ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado.

- **Vulnerabilidad categoría MEDIA #8**: SSL Medium Strength Cipher Suites Supported.

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la fuerza media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.
Tenga en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.
Solución: Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de resistencia media.

- **Vulnerabilidad categoría MEDIA #9** SSL Certificate Cannot Be Trusted

Descripción: El certificado X.509 del servidor no se puede confiar. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado auto firmado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando la exploración se produce antes de una de las fechas de "no antes" del certificado, o después de una de las fechas de "no después de" del certificado.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas erróneas se pueden arreglar al obtener el certificado con la firma errónea para que el emisor lo vuelva a firmar. Las firmas que no se pudieron verificar son el resultado del emisor del certificado que utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.

Solución: Compre o genere un certificado adecuado para este servicio.

- **Vulnerabilidad categoría MEDIA #10**: SSL Self-Signed Certificate

Descripción: La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificados reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquier persona podría establecer un ataque de hombre en el medio contra el host remoto.

Solución: Compre o genere un certificado adecuado para este servicio.

- **Vulnerabilidad categoría MEDIA #11**: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) (CVE-2014-3566).

Descripción: El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MITM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes encriptados usando cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC).

Los atacantes de MITM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256

intentos si pueden forzar a una aplicación víctima a enviar repetidamente los mismos datos a través de las conexiones SSL 3.0 recién creadas.

Solución: Deshabilitar SSLv3 es la única forma de mitigar completamente la vulnerabilidad.

- **IP = 172.18.46.190**

Para detectar las vulnerabilidades del servidor con IP 172.18.46.190, se seleccionó la herramienta de software NESSUS 8.0.0, y los resultados fueron los siguientes:

- 1 vulnerabilidades categoría CRITICA
- 0 vulnerabilidades categoría ALTA
- 5 vulnerabilidades categoría MEDIA
- 2 vulnerabilidades categoría BAJA

A continuación, se realiza un resumen de las principales vulnerabilidades encontradas y su análisis (1 categoría critica, 0 categoría alta, 5 categoría media).

- **Vulnerabilidad categoría CRÍTICA #1:** Microsoft Windows SMBv1 Multiple Vulnerabilities.

Descripción: El host remoto de Windows tiene Microsoft Server Message Block 1.0 (SMBv1) habilitado. Es, por lo tanto, afectado por múltiples vulnerabilidades:

- Existen múltiples vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para revelar información confidencial (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276).
- Existen múltiples vulnerabilidades de denegación de servicio en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de una solicitud SMB especialmente diseñada, para hacer que el sistema deje de responder (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280).
- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un

paquete SMBv1 especialmente diseñado, para ejecutar código arbitrario (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279).

Solución: Se debe aplicar la actualización de seguridad aplicable a la versión de Windows, para nuestro caso Windows Server 2012 R2 Standard, por tanto, sería la actualización KB4019215.

- **Vulnerabilidad categoría MEDIA #1**: SMB Signing not required

Descripción: La firma no es requerida en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediarios contra el servidor SMB. La firma SMB es un mecanismo de seguridad en el protocolo SMB. Por defecto, la firma SMB está deshabilitada. Cuando la firma SMB está habilitada en el sistema de almacenamiento, es el equivalente a la política del servidor de red de Microsoft "Firmar digitalmente las comunicaciones (si el cliente está de acuerdo)".

Solución: Imponer la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft: firmar comunicaciones digitalmente (siempre)'.

- **Vulnerabilidad categoría MEDIA #2**: SSL Certificate Signed Using Weak Hashing Algorithm (CVE-2004-2761).

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

Solución: La recomendación es ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado.

- **Vulnerabilidad categoría MEDIA #3**: SSL Medium Strength Cipher Suites Supported.

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera la fuerza media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Tenga en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.

Solución: Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de resistencia media.

- **Vulnerabilidad categoría MEDIA #4**: SSL Certificate Cannot Be Trusted.

Descripción: El certificado X.509 del servidor no se puede confiar. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado auto firmado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando la exploración se produce antes de una de las fechas de "no antes" del certificado, o después de una de las fechas de "no después de" del certificado.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas erróneas se pueden arreglar al obtener el certificado con la firma errónea para que el emisor lo vuelva a firmar. Las firmas que no se pudieron verificar son el resultado del emisor del certificado que utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.

Solución: Compre o genere un certificado adecuado para este servicio.

- **Vulnerabilidad categoría MEDIA #5**: SSL Self-Signed Certificate.

Descripción: La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificados reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquier persona podría establecer un ataque de hombre en el medio contra el host remoto.

Solución: Compre o genere un certificado adecuado para este servicio.

B. Interpretación de resultados de las pruebas de vulnerabilidades

Con base a las pruebas de vulnerabilidades realizadas en el capítulo anterior, podemos presentar un resumen del estado actual de los servidores de preproducción de la organización.

El escaneo de vulnerabilidades arrojó 178 servidores, en el segmento de red 172.18.46.0 con los siguientes resultados:

- Criticas: 45
- Altas: 106
- Medias: 668
- Bajas: 368
- Informativas: 7554

Para el respectivo análisis se tomaron en cuenta solo los servidores con al menos una vulnerabilidad con severidad crítica, resultando que de 178 servidores inicialmente solo sean materia de estudio 14 de ellos. En la figura 12 podemos visualizar una gráfica donde se presenta los niveles de criticidad discriminado por vulnerabilidad crítica, alta, media y baja de los 14 servidores que analizaremos en adelante.

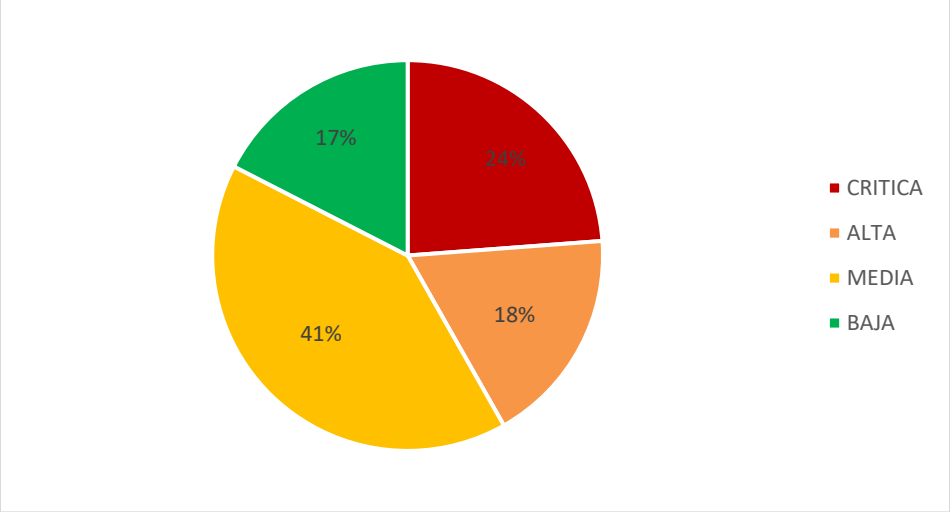


Figura 12: Niveles de severidad de las vulnerabilidades en los 14 servidores.

En la tabla 10 y figura 13 se presenta un panorama resumen del estado actual de los servidores que tuvieron vulnerabilidades críticas halladas por la herramienta NESSUS, permitiendo ver los equipos con mayores problemas de seguridad y que requieren de mayor atención.

HOST	NÚMERO DE VULNERABILIDADES					
	CRITICA	ALTA	MEDIA	BAJA	INFORMATIVA	TOTAL
172.18.46.72	13	2	3	2	36	56
172.18.46.103	7	1	3	2	32	45
172.18.46.33	4	2	0	1	27	34
172.18.46.178	3	13	29	2	51	98
172.18.46.97	2	4	15	4	114	139
172.18.46.28	2	2	2	1	37	44
172.18.46.163	2	2	4	2	53	63
172.18.46.126	2	1	5	2	46	56
172.18.46.224	2	1	0	3	44	50
172.18.46.226	2	1	0	3	43	49
172.18.46.229	2	1	0	3	36	42
172.18.46.230	2	1	0	3	36	42
172.18.46.53	1	3	11	3	76	94
172.18.46.190	1	0	5	2	60	68
TOTAL	45	34	77	33	691	880

Tabla 10: Resumen análisis de vulnerabilidades de servidores

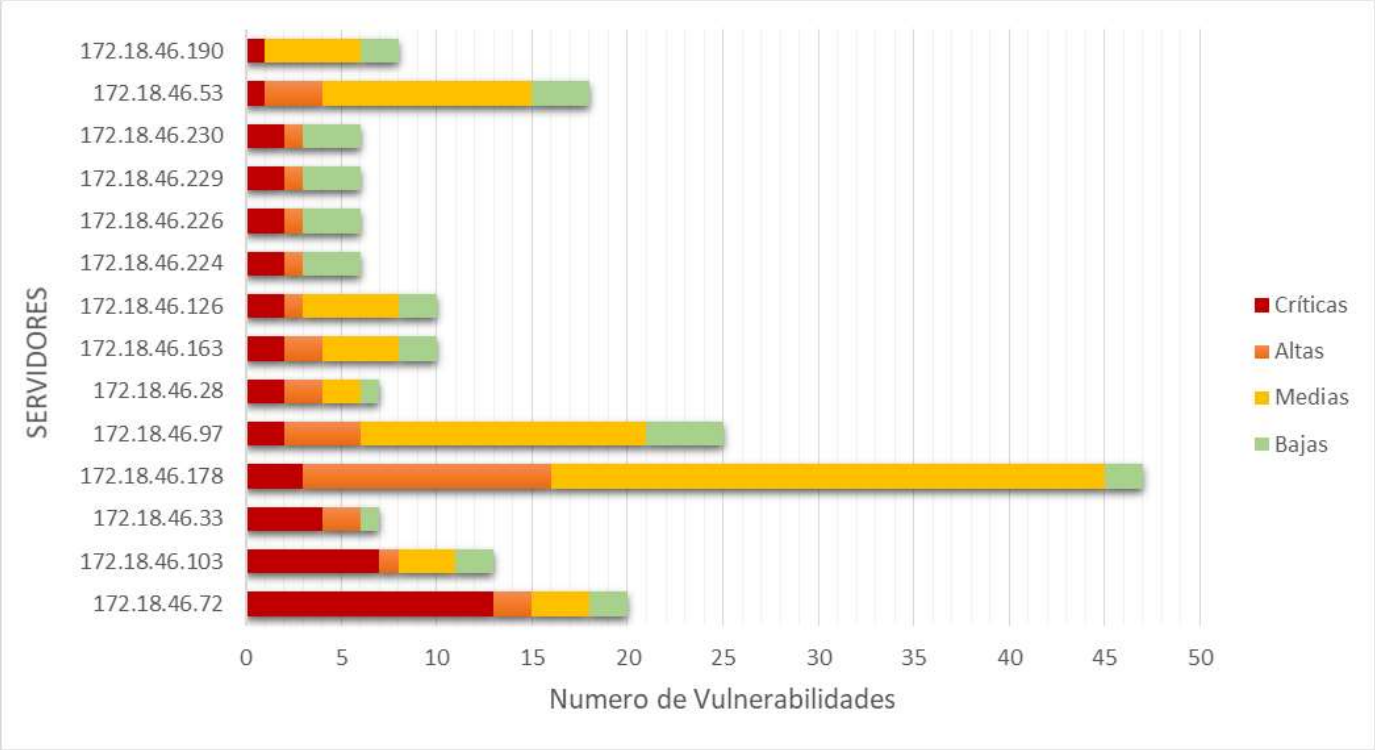


Figura 13: Barra análisis de vulnerabilidades

Con lo anterior se deduce que nuestro esfuerzo debe ir enfocado en los 14 servidores ya que tienen vulnerabilidades críticas y representan brechas de datos fácilmente explotables con preludios de inminentes ataques que pueden desembocar en impactos catastróficos.

En cifras hay un total de 45 vulnerabilidades críticas que corresponden al 24%, 34 vulnerabilidades altas con el 18% y 77 con severidad medias que conciernen al 41%, para un total de 156. Así mismo, que el servidor con dirección 172.18.46.72 es el que tiene mayor número de vulnerabilidades críticas y el servidor con dirección 72.18.46.178 es el que tienen más vulnerabilidades. Los anteriores datos preocupan por lo que deben controlarse con urgencia en la empresa, además que se encuentra en un nivel de riesgo MEDIO en sus servidores de preproducción.

10.5. Entrega de resultados

Luego de realizado el análisis detallado de los resultados en la fase anterior, se presentan los siguientes resultados:

- Matriz de vulnerabilidades y respuesta
- Análisis de la matriz de vulnerabilidades y respuesta
- Recomendaciones de seguridad

10.5.1. Matriz de vulnerabilidades y respuestas a los servidores

En la siguiente matriz de vulnerabilidades identificadas durante el desarrollo del análisis, se parte por indicar el dispositivo objeto de análisis, luego se lista el CVE (Common Vulnerabilities and Exposures) que identifica el número del boletín donde se encontrara más información de la vulnerabilidad, posteriormente el componente que se ejecuta en el host, el cual puede tener una o más vulnerabilidades, junto con la respuesta que se debe dar frente a la(s) misma(s) con el fin de mitigar o eliminar el riesgo existente, en seguida, se califica el impacto en términos de Confidencialidad (C), Integridad (I) y Disponibilidad (D), luego la complejidad de acceso o de ataque, posterior se señala los privilegios requeridos para explotar la vulnerabilidad y por último el puerto de ataque.

La matriz de vulnerabilidades que se muestra a continuación, en su columna puntaje CVSS (Common Vulnerability Scoring System), está la puntuación base CVSS versión 3 o versión 2, para

el caso de este último, en la columna CVS se precisa si es la versión 2 (ej. CVE-2010-0434 v2), para la versión 3 no se especifica este dato. Es importante mencionar que una vulnerabilidad puede estar calificada con la versión 3 y versión 2, si fuera así, tomaríamos como valor la versión 3, además que la puntuación base CVSS en la mayoría de los casos son diferentes, dado que las métricas de cálculos son distintas, por ejemplo la vulnerabilidad con CVE-2017-7679, cuenta con CVSS v3.0 con puntuación base 9.8 CRITICAL y CVSS v2.0 con puntuación base 7.5 HIGH.

El CVSS v3 y v2 tiene las siguientes métricas para generar la puntuación base:

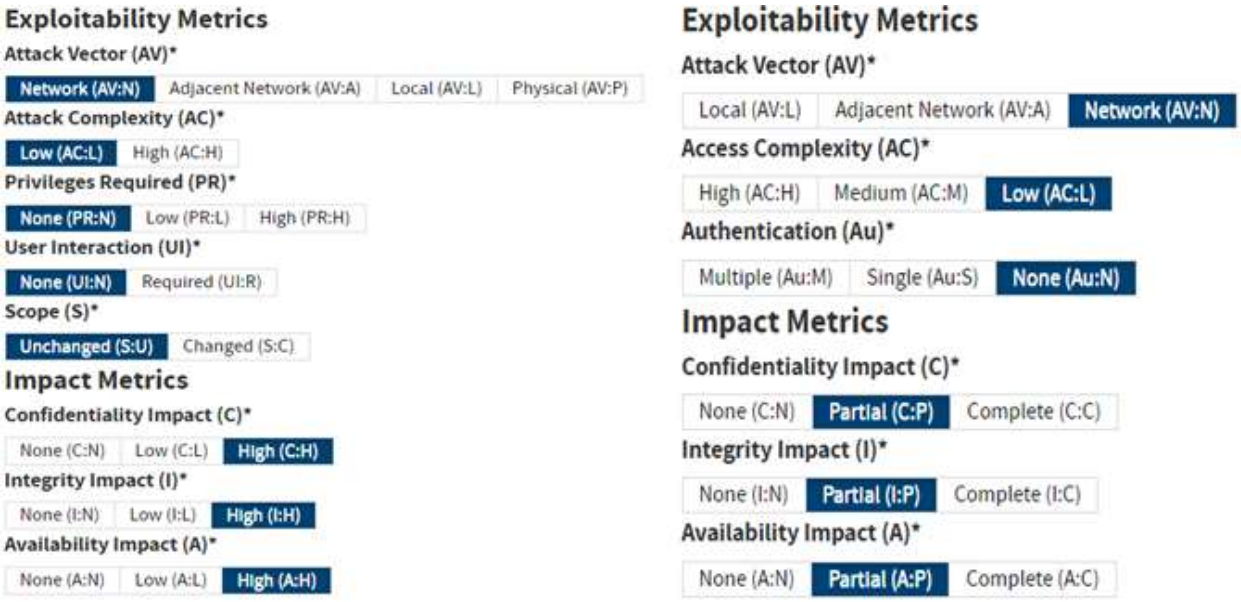


Figura 14: Métricas CVSS v3 vs CVSS v2

MATRIZ DE VULNERABILIDADES Y RESPUESTA A LOS SERVIDORES

Host	CVE	Puntaje CVSS	Categoría Vulnerabilidad	Componente Vulnerable	Respuesta	Impacto			Complejidad de Ataque	Privilegios Requeridos	Puerto
						C	I	D			
172.18.46.72	CVE-2015-4852	9.8	CRÍTICA	Oracle WebLogic Java Object Deserialization RCE.	Actualizar a la versión según el aviso de Oracle.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 – TCP/9006
	CVE-2016-0638	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU).	Aplicar el parche adecuado de acuerdo con el aviso de actualización de Oracle de abril de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 - TCP/9006
	CVE-2016-3510	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU).	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 - TCP/9006
	CVE-2016-5535	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU).	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 - TCP/9006
	CVE-2017-3248	9.8	CRÍTICA	Oracle WebLogic Server Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU).	Aplique el parche adecuado de acuerdo con la remediación de actualización de enero de 2017.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 - TCP/9006

	CVE-2017-10271	9.8	CRÍTICO	Oracle WebLogic WSAT Code Execution	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2017.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004
	CVE-2018-2628	9.8	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 - TCP/9006
	CVE-2018-2893	9.8	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7004 – TCP/9006
172.18.46.103	CVE-2015-4852	9.8	CRÍTICA	Oracle WebLogic Java Objetc Desealization RCE	Actualizar a la versión según el aviso de Oracle.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2016-0638	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU).	Aplicar el parche adecuado de acuerdo con el aviso de actualización de Oracle de abril de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2016-3510	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU).	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002

	CVE-2016-5535	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU).	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2016.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2017-3248	9.8	CRÍTICA	Oracle WebLogic Server Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU).	Aplique el parche adecuado de acuerdo con la remediación de actualización de enero de 2017.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2017-10271	9.8	CRÍTICA	Oracle WebLogic WSAT Code Execution	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de octubre de 2017.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2018-2628	10.0	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
	CVE-2018-2893	9.8	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/7002
172.18.46.33	CVE-2016-5535	9.8	CRÍTICA	Oracle WebLogic Server Java Object Deserialization	Aplique el parche adecuado de acuerdo con el aviso de	Alto	Alto	Alto	Bajo	Ninguno	TCP/9000 – TCP/9001

				RCE (October 2016 CPU).	actualización de parche crítico de octubre de 2016.						
	CVE-2018-2628	10.0	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Aplique el parche adecuado de acuerdo con el aviso de actualización de parche crítico de Oracle de abril de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/9000 - TCP/9001
	CVE-2018-2893	9.8	CRÍTICA	Oracle WebLogic Server Deserialization RCE	Se debe aplicar el parche adecuado de acuerdo con el aviso de actualización de parche crítico de julio de 2018.	Alto	Alto	Alto	Bajo	Ninguno	TCP/9000 – TCP/9001
172.18.46.178	CVE-2010-0434 v2	4.3	MEDIA	Apache 2.2.x < 2.2.15 Vulnerabilidades múltiples.	Actualiza a la versión 2.2.15 de Apache o posterior.	Parcial	Nada	Nada	Medio	Ninguno	TCP/80
	CVE-2007-6750, CVE-2010-0408 v2	5.0	MEDIA	Apache 2.2.x < 2.2.15 Vulnerabilidades múltiples.	Actualiza a la versión 2.2.15 de Apache o posterior.	Nada	Nada	Parcial	Bajo	Ninguno	TCP/80
	CVE-2009-3555 v2	5.8	MEDIA	Apache 2.2.x < 2.2.15 Vulnerabilidades múltiples.	Actualiza a la versión 2.2.15 de Apache o posterior.	Nada	Parcial	Parcial	Medio	Ninguno	TCP/80
	CVE-2010-0425 v2	10.0	CRÍTICA	Apache 2.2.x < 2.2.15 Vulnerabilidades múltiples.	Actualiza a la versión 2.2.15 de Apache o posterior.	Completo	Completo	Completo	Bajo	Ninguno	TCP/80
	CVE-2009-2412 v2	10.0	CRÍTICA	Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow	Actualizar a Apache 2.2.13 o posterior.	Completo	Completo	Completo	Bajo	Ninguno	TCP/80

	Sin CVE	10.0	CRÍTICA	PHP Unsupported Version Detection	Actualiza a una versión de PHP que actualmente es compatible.	Completo	Completo	Completo	Bajo	Ninguno	TCP/80
	CVE-2007-4850 v2	5.0	MEDIA	PHP < 5.2.6 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.2.6 o posterior.	Parcial	Ninguno	Ninguno	Bajo	Ninguno	TCP/80
	CVE-2007-6039 v2	2.1	BAJA	PHP < 5.2.6 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.2.6 o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-0599 v2	10.0	CRÍTICA	PHP < 5.2.6 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.2.6 o posterior.	Completo	Completo	Completo	Bajo	Ninguno	TCP/80
	CVE-2008-1384 v2	5.0	MEDIA	PHP < 5.2.6 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.2.6 o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-2050, CVE-2008-2051 v2	10.0	CRÍTICA	PHP < 5.2.6 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.2.6 o posterior.	Completo	Completo	Completo	Insuficiente información	Ninguno	TCP/80
	Sin CVE	10.0	CRÍTICA	Unsupported Web Server Detection	Eliminar el servicio si no es necesario. De lo contrario, actualice a una versión más nueva.	Alto	Alto	Alto	Bajo	Ninguno	TCP/80
	CVE-2008-2371 v2	7.5	ALTA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-2665, CVE-2008-2666, CVE-2008-2829 v2	5.0	MEDIA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Parcial	Ninguno	Ninguno	Bajo	Ninguno	TCP/80

	CVE-2008-3658, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-8626 v2	7.5	ALTA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-3659 v2	6.4	MEDIA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Ninguno	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-3660 v2	5.0	MEDIA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-5557 v2	10.0	CRÍTICA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Completo	Completo	Completo	Bajo	Ninguno	TCP/80
	CVE-2008-7068 v2	6.4	MEDIA	PHP 5 < 5.2.7 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior. Tenga en cuenta que la versión 5.2.7 se ha eliminado de la distribución.	Ninguno	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2008-5814 v2	2.6	BAJA	PHP 5 < 5.2.8 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior.	Ninguno	Parcial	Ninguno	Alto	Ninguno	TCP/80

	CVE-2008-5844, CVE-2009-4018 v2	7.5	ALTA	PHP 5 < 5.2.8 Multiple Vulnerabilities	Actualiza a la versión 5.2.8 de PHP o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2009-3291-3293 v2	7.5	ALTA	PHP 5 < 5.2.11 Multiple Vulnerabilities	Actualiza a la versión de PHP 5.2.11 o posterior.	Parcial	Parcial	Parcial	Información insuficiente	Ninguno	TCP/80
	CVE-2009-5016 v2	6.8	MEDIA	PHP 5 < 5.2.11 Multiple Vulnerabilities	Actualiza a la versión de PHP 5.2.11 o posterior.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/80
	CVE-2009-3294 v2	5.0	MEDIA	PHP 5 < 5.2.11 Multiple Vulnerabilities	Actualiza a la versión de PHP 5.2.11 o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2009-2699 v2	5.0	MEDIA	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2009-3094 v2	2.6	BAJA	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Ninguno	Ninguno	Parcial	Alto	Ninguno	TCP/80
	CVE-2009-3095 v2	7.5	ALTA	Apache 2.2.x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2007-1581 v2	9.3	CRÍTICA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Completo	Completo	Completo	Medio	Ninguno	TCP/80
	CVE-2010-0397, CVE-2010-3065 v2	5.0	MEDIA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-	5.0	MEDIA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Parcial	Ninguno	Ninguno	Bajo	Ninguno	TCP/80

	2190, CVE-2010-2484 v2										
	CVE-2010-2191 v2	6.4	MEDIA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Parcial	Parcial	Ninguno	Bajo	Ninguno	TCP/80
	CVE-2010-2225 v2	7.5	ALTA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2010-2531 v2	4.3	MEDIA	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Actualizar a la versión 5.2.14 de PHP o posterior.	Parcial	Ninguno	Ninguno	Medio	Ninguno	TCP/80
	CVE-2011-3379 v2	7.5	ALTA	PHP < 5.3.9 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.9 o posterior.	Ninguno	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2011-4566 v2	6.4	MEDIA	PHP < 5.3.9 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.9 o posterior.	Parcial	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2011-4885, CVE-2012-0781, CVE-2012-0788, CVE-2012-0789 v2	5.0	MEDIA	PHP < 5.3.9 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.9 o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2011-4566 v2	6.4	MEDIA	PHP 5.2 < 5.3.9 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.9 o posterior.	Parcial	Parcial	Ninguno	Bajo	Ninguno	TCP/80
	CVE-2011-1398 v2	4.3	MEDIA	PHP 5.2 < 5.3.11 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.11 o posterior.	Ninguno	Parcial	Ninguno	Medio	Ninguno	TCP/80
	CVE-2012-0831 v2	6.8	MEDIA	PHP 5.2 < 5.3.11 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.11 o posterior.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/80
	CVE-2012-1172 v2	5.8	MEDIA	PHP 5.2 < 5.3.11 Multiple Vulnerabilities	Actualizar a la versión de PHP 5.3.11 o posterior.	Ninguno	Parcial	Parcial	Medio	Ninguno	TCP/80

	CVE-2012-1823 v2	7.5	ALTA	PHP < 5.3.12 / 5.4.2 CGI String Excute	Actualice a la versión de PHP 5.3.12 / 5.4.2 o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
	CVE-2013-5704 v2	5.0	MEDIA	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Actualiza a la versión 2.2.29 de Apache o posterior.	Ninguno	Parcial	Ninguno	Bajo	Ninguno	TCP/80
	CVE-2014-0118 v2	4.3	MEDIA	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Actualiza a la versión 2.2.29 de Apache o posterior.	Ninguno	Ninguno	Ninguno	Medio	Ninguno	TCP/80
	CVE-2014-0226 v2	6.8	MEDIA	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Actualiza a la versión 2.2.29 de Apache o posterior.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/80
	CVE-2014-0231 v2	5.0	MEDIA	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Actualiza a la versión 2.2.29 de Apache o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2017-3167, CVE-2017-3167, CVE-2017-7668, CVE-2017-7679	9.8	CRÍTICA	Apache 2.2.x < 2.2.33-dev /2.4.x < 2.4.26 Multiple Vulnerabilities	Actualice a Apache versión 2.2.33-dev / 2.4.26 o posterior.	Alto	Alto	Alto	Bajo	Ninguno	TCP/80
	CVE-2017-7659	7.5	ALTA	Apache 2.2.x < 2.2.33-dev /2.4.x < 2.4.26 Multiple Vulnerabilities	Actualice a Apache versión 2.2.33-dev / 2.4.26 o posterior.	Ninguno	Ninguno	Alto	Bajo	Ninguno	TCP/80
	CVE-2017-3167, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679	9.8	CRÍTICA	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities	Actualiza a la versión 2.2.34 de Apache o posterior.	Alto	Alto	Alto	Bajo	Ninguno	TCP/80
	CVE-2017-9788	9.1	CRÍTICA	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities	Actualiza a la versión 2.2.34 de Apache o posterior.	Alto	Ninguno	Alto	Bajo	Ninguno	TCP/80

	CVE-2009-2699 v2	5.0	MEDIA	Apache 2.2x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Ninguno	Ninguno	Parcial	Bajo	Ninguno	TCP/80
	CVE-2009-3094 v2	2.6	BAJA	Apache 2.2x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Ninguno	Ninguno	Parcial	Alta	Ninguno	TCP/80
	CVE-2009-3095 v2	7.5	ALTA	Apache 2.2x < 2.2.14 Multiple Vulnerabilities	Actualiza a la versión 2.2.14 de Apache o posterior.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/80
172.18.46.97	CVE-2007-1036 v2	7.5	ALTA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Si usa EMC Data Protection Advisor, actualice a la versión 6.xo aplique la solución alternativa a 5.x. o elimine cualquier servlet JBoss afectado.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/9080
	CVE-2012-0874, CVE-2012-0874 v2	6.8	MEDIA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Si usa EMC Data Protection Advisor, actualice a la versión 6.xo aplique la solución alternativa a 5.x. o elimine cualquier servlet JBoss afectado.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/9080
	CVE-2013-4810	10.0	CRÍTICA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Si usa EMC Data Protection Advisor, actualice a la versión 6.xo aplique la solución alternativa a 5.x. o elimine cualquier servlet JBoss afectado.	Alto	Alto	Alto	Bajo	Ninguno	TCP/9080

	CVE-2015-7501	9.8	CRÍTICA	JBoss Java Object Deserialization RCE	Se debe actualizar de acuerdo a lo que ordena Apache commons-collections	Alto	Alto	Alto	Bajo	Ninguno	TCP/9080
	Sin CVE	-	ALTA	SSL Version 2 and 3 Protocol Detection	Deshabilitar SSL 2.0 y 3.0 y en lugar utilizar TLS 1.1 o superior, en conjunto con cifrados aprobados.	-	-	-	-	-	TCP/443
	CVE-2017-12149	9.8	CRÍTICA	JBoss Enterprose Application Platform doFilter() Method Insecure Deserialization RCE	Asegure el acceso a todos los contextos de http-invoker agregando <url-pattern> / * </url-pattern> a las restricciones de seguridad en el archivo web.xml de http-invoker.sar.	Alto	Alto	Alto	Bajo	Ninguno	TCP/8380 – TCP/9080
	Sin CVE v2	7.5	ALTA	Jboss JMX Console Unrestricted Access	Asegure o elimine el acceso a JMX y / o la consola web utilizando las opciones de instalación avanzadas.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/9080
172.18.46.28	CVE-2007-1036 v2	7.5	ALTA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x	Parcial	Parcial	parcial	Bajo	Ninguno	TCP/8180

	CVE-2012-0874 v2	6.8	MEDIA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x	Parcial	Parcial	Parcial	Medio	ninguno	TCP/8180
	CVE-2013-4810	10.0	CRÍTICA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x	Alto	Alto	Alto	Bajo	Ninguno	TCP/8180
	CVE-2012-0874 v2	6.8	MEDIA	JBoss Java Object Deserialization RCE	Aplique el parche adecuado de acuerdo con el aviso del proveedor. Alternativamente, asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss estén protegidos por firewall desde cualquier red pública.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/8180
	CVE-2015-7501	9.8	CRÍTICA	JBoss Java Object Deserialization RCE.	Aplique el parche adecuado de acuerdo con el aviso del proveedor. Alternativamente, asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss	Alto	Alto	Alto	Bajo	Ninguno	TCP/8180

					estén protegidos por firewall desde cualquier red pública.						
	CVE-2007-1036 v2	7.5	ALTA	JBoss JMX Console Unrestricted Access	Asegure o elimine el acceso a JMX o la consola web utilizando las opciones de instalación avanzadas.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/8180
	CVE-2017-12149	9.8	CRÍTICA	JBoss Enterprise Application Platform do Filter Method Insecure Deserialization RCE.	Siga las pautas de mitigación proporcionadas en el aviso de Red Hat.	Alto	Alto	Alto	Bajo	Ninguno	TCP/8180
172.18.46.163	CVE-2007-1036 v2	7.5	ALTA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x o elimine cualquier servlet JBoss afectado.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/8180
	CVE-2012-0874 v2	6.8	MEDIA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x o elimine cualquier servlet JBoss afectado.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/8180
	CVE-2013-4810 v2	10.0	CRÍTICA	Apache Tomcat /JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities	Se debe actualizar a la actualizar a la versión 6.x o elimine cualquier servlet JBoss afectado.	Completo	Completo	Completo	Bajo	Ninguno	TCP/8180

	CVE-2012-0874 v2	6.8	MEDIA	JBoss Java Objetc Deserialization RCE.	Asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss estén protegidos por firewall desde cualquier red pública.	Parcial	Parcial	Parcial	Medio	Ninguno	TCP/8180
	CVE-2015-7501	9.8	CRÍTICA	JBoss Java Object Deserialization RCE.	Asegúrese de que todos los puertos expuestos utilizados por el servidor JBoss estén protegidos por firewall desde cualquier red pública.	Alto	Alto	Alto	Bajo	Ninguno	TCP/8180
	CVE-2007-1036 v2	7.5	ALTA	JBoss JMX Console Unrestricted Access	Asegure o elimine el acceso a JMX o la consola web utilizando las opciones de instalación avanzadas.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/8180
	CVE-2017-12149	9.8	CRÍTICA	JBoss Enterprise Application Platform do Filter Method Insecure Deserialization RCE.	Siga las pautas de mitigación proporcionadas en el aviso de Red Hat.	Alto	Alto	Alto	Bajo	Ninguno	TCP/8180
172.18.46.126	Sin CVE	10.0	CRÍTICA	HP Data Protector Unsupported	Actualice a una versión de HP Data Protector que actualmente es compatible.	Completo	Completo	Completo	Bajo	Ninguno	TCP/5555

	CVE-2013-2344 – 2350, CVE-2013-6194 – 6195 v2	10.0	CRÍTICA	HP Data Protector Multiple Vulnerabilities	Actualice a una versión de HP Data Protector que actualmente es compatible.	Completo	Completo	Completo	Bajo	Ninguno	TCP/5555
	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513
172.18.46.224	CVE-1999-0526 v2	10.0	CRÍTICA	X11 Server Unauthenticated Access	Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001
	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access: Screenshot	Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001
	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513

					servicio y use SSH en su lugar.						
172.18.46.226	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access	Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.	Completa	Completa	Completa	Bajo	Ninguno	TCP/6001
	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access: Screenshot	Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001
	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513
172.18.46.229	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access	Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001

	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access: Screenshot	Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001
	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513
172.18.46.230	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access	Restrinja el acceso a este puerto mediante el comando 'xhost'. Si no se utiliza la instalación cliente / servidor X11, desactive TCP por completo.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001
	CVE-1999-0526 v2	10.0	CRÍTICA	X Server Unauthenticated Access: Screenshot	Restrinja el acceso a puertos mediante el comando 'xhost'. Si no se utiliza la instalación de cliente servidor, desactive completamente las conexiones TCP al servidor.	Completo	Completo	Completo	Bajo	Ninguno	TCP/6001

	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513
172.18.46.53	CVE-1999-0618 v2	10.0	CRÍTICA	Rexecd Service Detection	Comente la línea 'exec' en /etc/inetd.conf y reinicie el proceso inetd.	Completo	Completo	Completo	Bajo	Ninguno	TCP/512
	CVE-1999-0651 v2	7.5	ALTA	rlogin Service Detection	Comente la línea de 'inicio de sesión' en /etc/inetd.conf y reinicie el proceso inetd. Alternativamente, deshabilite este servicio y use SSH en su lugar.	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/513
	CVE-2012-1675 v2	7.5	ALTA	Oracle TNS Listener Remote Poisoning	Las recomendaciones para protegerse de esta vulnerabilidad se puede encontrar en Oracle Support Note 1340831.1	Parcial	Parcial	Parcial	Bajo	Ninguno	TCP/1521
	Sin CVE	-	ALTA	SSL Version 2 and 3 Protocol Detection	Deshabilitar SSL 2.0 y 3.0 y en lugar utilizar TLS 1.1 o superior, en conjunto con cifrados aprobados.	-	-	-	-	-	TCP/5989

172.18.46.190	CVE-2017-0267 – 0271, CVE-2017-0273 – 0276, CVE-2017-0280	5.9	MEDIA	Microsoft Windows SMBv1 Multiple Vulnerabilities	Se debe aplicar la actualización de seguridad aplicable a la versión de Windows, para nuestro caso Windows Server 2012 R2 Standard, por tanto, sería la actualización KB4019215.	Alto	Ninguno	Ninguno	Alto	Ninguno	TCP/445
	CVE-2017-0272	8.1	ALTO	Microsoft Windows SMBv1 Multiple Vulnerabilities	Se debe aplicar la actualización de seguridad aplicable a la versión de Windows, para nuestro caso Windows Server 2012 R2 Standard, por tanto, sería la actualización KB4019215.	Alto	Alto	Alto	Alto	Ninguno	TCP/445
	CVE-2017-0277 - 0279	7.0	ALTO	Microsoft Windows SMBv1 Multiple Vulnerabilities	Se debe aplicar la actualización de seguridad aplicable a la versión de Windows, para nuestro caso Windows Server 2012 R2 Standard, por tanto, sería la actualización KB4019215.	Alto	Bajo	Bajo	Alto	Ninguno	TCP/445

10.5.2. Análisis de la matriz de vulnerabilidades y respuesta

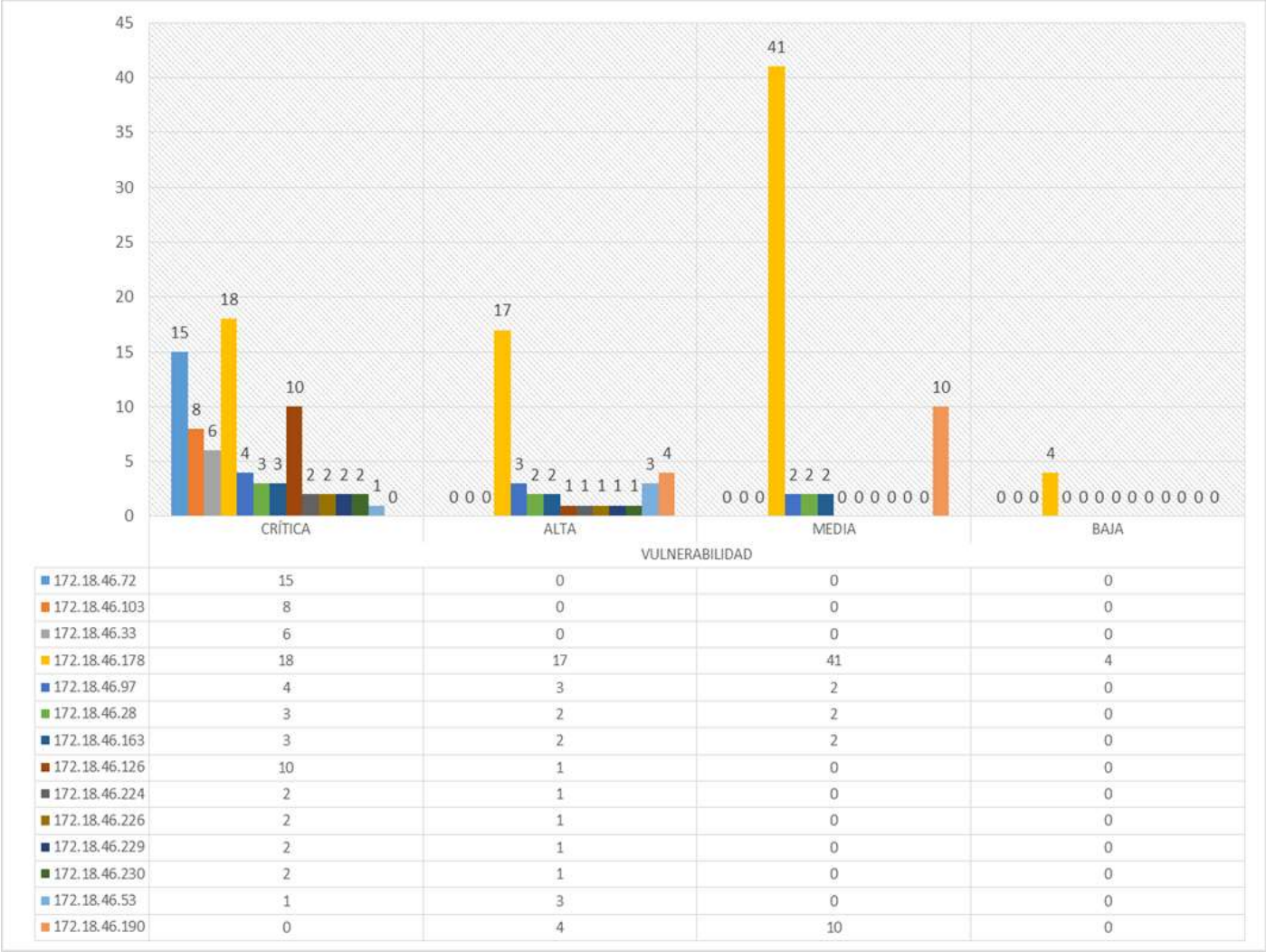
La anterior matriz se realizó con las vulnerabilidades CRÍTICAS y ALTAS que arrojo la herramienta NESSUS, pero se puede apreciar que primero, cada componente puede tener uno o más vulnerabilidades y segundo, que el hecho de que la herramienta califique a un componente con múltiples vulnerabilidades, no significa que todas las vulnerabilidades de ese componente tenga la misma severidad y puntaje.

Una de las columnas más importantes de la matriz es el impacto a nivel de Confidencialidad, Integridad y Disponibilidad que tienen actualmente cada servidor, siendo el impacto Alto/Completo con los de mayor número (claro está que es natural estos valores, dado que analizamos las vulnerabilidades críticas y altas), además, que la Confidencialidad con impacto Alto/Completo fue el atributo de la seguridad con la cifra más alta. Al mismo tiempo, que el servidor con dirección IP 172.18.46.178 es el activo con mayor impacto en términos de seguridad digital.

HOST	IMPACTO								
	Confidencialidad			Integridad			Disponibilidad		
	Alto/Completo	Bajo/Parcial	Ninguno/Nada	Alto/Completo	Bajo/Parcial	Ninguno/Nada	Alto/Completo	Bajo/Parcial	Ninguno/Nada
172.18.46.72	15	0	0	15	0	0	15	0	0
172.18.46.103	8	0	0	8	0	0	8	0	0
172.18.46.33	6	0	0	6	0	0	6	0	0
172.18.46.178	18	36	26	17	29	34	19	41	20
172.18.46.97	4	3	0	4	3	0	4	3	0
172.18.46.28	3	4	0	3	4	0	3	4	0
172.18.46.163	3	4	0	3	4	0	3	4	0
172.18.46.126	10	1	0	10	1	0	10	1	0
172.18.46.224	2	1	0	2	1	0	2	1	0
172.18.46.226	2	1	0	2	1	0	2	1	0
172.18.46.229	2	1	0	2	1	0	2	1	0
172.18.46.230	2	1	0	2	1	0	2	1	0
172.18.46.53	1	2	0	1	2	0	1	2	0
172.18.46.190	14	0	0	1	3	10	1	3	10
TOTAL	90	54	26	76	50	44	78	62	30

Tabla 11: Impacto de las vulnerabilidades en cada servidor

En la figura 15, se observa los servidores en estudio con todos los niveles de gravedad (crítica, alta, media y baja) de los componentes que la herramienta NESSUS los presento con severidad CRÍTICA y ALTA; cabe recordar que un componente instalado en un activo puede tener múltiples vulnerabilidades, las cuales pueden tener diferentes niveles de gravedad.



	CRÍTICA	ALTA	MEDIA	BAJA
172.18.46.72	15	0	0	0
172.18.46.103	8	0	0	0
172.18.46.33	6	0	0	0
172.18.46.178	18	17	41	4
172.18.46.97	4	3	2	0
172.18.46.28	3	2	2	0
172.18.46.163	3	2	2	0
172.18.46.126	10	1	0	0
172.18.46.224	2	1	0	0
172.18.46.226	2	1	0	0
172.18.46.229	2	1	0	0
172.18.46.230	2	1	0	0
172.18.46.53	1	3	0	0
172.18.46.190	0	4	10	0

Figura 15: Niveles de gravedad de todas las CVE de las vulnerabilidades críticas y altas

La figura 16, indica que en la matriz hay 173 vulnerabilidades, de las cuales, su complejidad de ataque en su mayoría es Bajo, con 133 casos (77%), seguido de nivel Alto con 17 casos (10%), luego de nivel Medio con 16 (9%), y por último, 7 vulnerabilidades que no reportaron información que equivale al 4%. La complejidad de ataque del 77% indica que se requiere muy poco conocimiento o habilidad para explotar la vulnerabilidad.

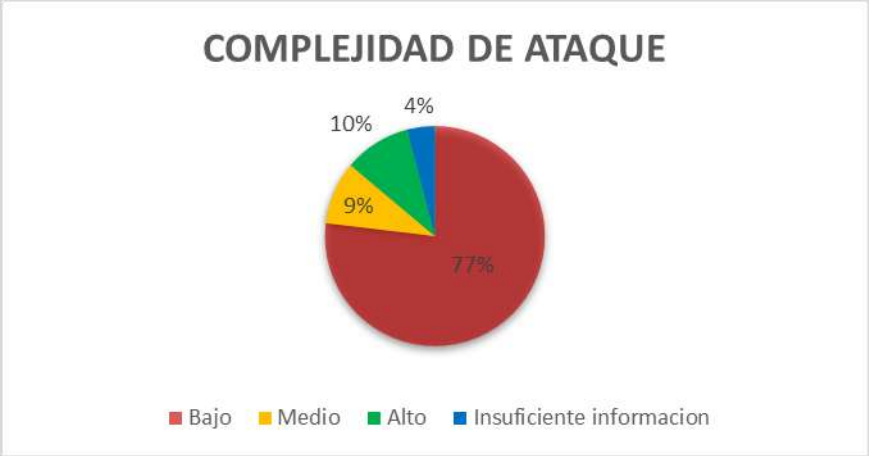


Figura 16: Complejidad de ataque de las vulnerabilidades críticas y altas.

10.5.3. Recomendaciones de seguridad

Con base en los resultados y análisis realizados a lo largo del proyecto, los integrantes del grupo hacen las siguientes recomendaciones de seguridad a la empresa Keralty:

- ✓ Se sugiere que las direcciones orígenes no reconocidas que estén asociadas a los eventos detectados por el IPS sean bloqueados por medio del Black_list del Firewall.

- ✓ Se recomienda, ejecutar un escaneo de vulnerabilidades sobre toda la infraestructura crítica para disminuir el riesgo de compromiso y cerrar brechas de seguridad más comunes.

- ✓ Se recomienda, analizar la posibilidad de la implementación de un sistema de protección de aplicaciones web (WAF) para el portal https://www.keralty.com. De esta manera, se agregaría un nivel más de protección al sitio web (seguridad por capas). El WAF está en la capacidad de proteger de ataques aún más elaborados que los ya han sido bloqueados por el módulo IPS que se tiene implementado actualmente pero que técnicamente, supera sus cualidades de protección.

- ✓ Se recomienda, realizar pruebas de ethical hacking al portal https://www.keralty.com, desactivando la protección del IPS, para detectar y remediar vulnerabilidades antes de que puedan ser explotadas por un atacante que haya podido evadir la protección del IPS (Deep Security). De esta manera, se pueden elevar los niveles de seguridad del portal y

por ende hacerlo más resistente a un ataque.

- ✓ Se recomienda la implementación de un servicio de monitoreo de seguridad a través de un CSOC, que permita la revisión y atención de eventos, atención de alertas e incidentes de manera proactiva. De esta manera, el tiempo de reacción ante cualquier situación inesperada de seguridad seria óptimo.
  Adicionalmente, se recomienda, la implementación de monitoreo proactivo de ciberamenazas apalancado en un SOC (ciberinteligencia) para estar atentos ante cualquier campaña de malware, ataques de denegación de servicio, explotación de vulnerabilidades a gran escala, etc., que puedan afectar a KERALTY.

- ✓ Debido a la ampliación de la cobertura que se tiene presupuestada, se recomienda realizar la implementación de un servicio Anti DDoS, el cual servirá para evitar indisponibilidades de los servicios web, ya que, al aumentar el tráfico de solicitudes, se pueden ver asociadas peticiones maliciosas por medio de agotamiento de protocolo o aumento de solicitudes.

- ✓ Como complemento a los controles sugeridos, se recomienda la adquisición de un servicio de reportes interactivos, el cual permite tener un Dashboard que contiene un consolidado de los eventos asociados a las plataformas de seguridad, esto facilitaría el análisis, para la toma de decisiones asociadas a seguridad que beneficiarían al negocio.

- ✓ Los incidentes de seguridad impactan en forma cada vez más directa sobre los activos estratégicos de la compañía, en consecuencia, es importante no solamente implementar controles técnicos sino efectivas acciones de concientización, capacitación, y difusión de mejores prácticas.

11. Resultados

Los resultados encontrados de acuerdo con los requerimientos planteados se describen en la siguiente tabla:

PASOS	REQUERIMIENTOS	RESULTADO FINAL
FASE 1	Analizar el estado actual de la compañía, identificar sus recursos y cómo es su estructura tecnológica.	Se realiza un levantamiento de información e inventario de equipos en conjunto con los administradores de red, así como el diseño de diagramas topológicos actualizados.
	Asimilar el negocio de la compañía, con el fin de encontrar sistemas críticos y que necesiten una especial atención.	El core de Keralty son los servicios prepagados y subsidiados de salud, dando criticidad a servidores transaccionales y bases de datos con información clasificada de pacientes.
	Estudiar el organigrama de la compañía, determinar los responsables de los sistemas que se van a evaluar y conocer su funcionamiento los procedimientos de los recursos tecnológicos de la compañía.	Se plantea aplicar esfuerzos en la corrección y aplicación de buenas prácticas sobre el firewall para disminuir el número de vulnerabilidades en la red y una vez finalizado se lanza análisis de vulnerabilidades.
	Agrupar documentos en donde se expliquen políticas, procesos y procedimientos que vayan apuntados a la seguridad informática y de la información en la compañía.	Verificando los procesos gestión de la documentación se organiza cronogramas y matriz de riesgos usando practicas utilizadas de buenos procesos de gestión documental.
FASE 2	Identificar y aclarar el alcance que la compañía permita para realizar un escáner de vulnerabilidades y equipos que permitan ser evaluados y corregidos.	Después de la reunión hecha con el director de infraestructura permite la corrección aplicación de buenas prácticas en el firewall y el análisis de vulnerabilidades sobre servidores en ambiente de preproducción
	Seleccionar las herramientas que se van a usar para la identificación de vulnerabilidades en todos los sistemas previamente seleccionados.	Se usó guía de hardenig fotigate brindado por el fabricante, software Nmap y Nessus, software plataforma excel parámetro de análisis de riesgos.

	Establecer un cronograma de actividades que no afecten la actividad del negocio.	Se realizó un pequeño cronograma de actividades para conocer las fechas y los tiempos que nos tomarían cada acción.
	Presentar el cronograma de actividades a la empresa con el fin de obtener su consentimiento.	Después de expuesto el plan de trabajo fue aceptado consecutivamente el cronograma de actividades por el director de infraestructura con fecha de inicio a partir del mes de abril.
FASE 3	Realizar análisis preventivos, basados en guías de hardening sobre firewall existente en la compañía.	Se realiza análisis sobre configuración de firewall, se identifican falencia a la hora de aprovechar al máximo el firewall.
	Aplicar plan correctivo sobre firewall Fortigate con estándar de buenas prácticas.	Se realizan acciones correctivas sobre firewall de acuerdo con guía de hardening
	Realizar la instalación de herramientas de identificación de vulnerabilidades en un ambiente controlado, sin riesgo de afectar el negocio y que sea aprobado por la empresa.	Con la autorización de la compañía y el visto bueno del director de infraestructura, en la fecha autorizada se da inicio a instalación en la red las herramientas anteriormente NESSUS y NMAP con el fin de generar informe de vulnerabilidades estando dentro de los dominios de red, una vez culminadas se inicia el proceso de análisis.
	Ejecutar el cronograma de actividades de identificación de vulnerabilidades en los sistemas previamente seleccionados.	
	Realizar pruebas a los servicios afectados, con el fin de comprobar su correcto funcionamiento.	
	Recopilar toda la información y resultados de las herramientas usadas para la identificación de vulnerabilidades.	La información está en los adjuntos entregados con este proyecto, en donde se almacenó los resultados arrojados por las herramientas de vulnerabilidades.

FASE 4	Identificar todas las vulnerabilidades críticas encontradas en la fase de escáner.	Posterior al análisis de cada vulnerabilidad encontrada, se guardó un registro documental que posteriormente fue incorporado en el documento final del proyecto de grado y documento dirigido entregado a ing. administrador de infraestructura de la empresa Keralty.
	Investigar el impacto de las vulnerabilidades encontradas en los sistemas críticos del negocio.	
	Determinar cuáles son las soluciones viables a las vulnerabilidades críticas o como se pueden mitigar.	
FASE 5	Elaborar un documento donde se expongan los resultados del análisis efectuado en la fase anterior.	El documento final del proyecto se presenta al director y jurados de grado como Especialista en Seguridad de Redes Telemáticas de la Universidad el Bosque y al jefe de infraestructura de Keralty.
	En el documento sobresalen las vulnerabilidades críticas que tengan una mayor probabilidad de ocurrencia y tengan el potencial de afectar seriamente al negocio.	
	El documento elaborado contiene recomendaciones hacia la empresa para reforzar su seguridad y prevenir un impacto negativo al negocio.	

Tabla 12: Requerimientos y resultados finales

12. Discusión

En base a las necesidades descubiertas existe un gran número de opciones de seguridad con capacidad de cubrir todas las necesidades de seguridad. Proteger la infraestructura de Keralty no se trata únicamente de instalar un antivirus en los ordenadores o de configurar bien las políticas del firewall, la protección debe ser más amplia y cubrir todos los ámbitos de la operativa y la gestión de datos de la compañía.

La información que debe protegerse ayudará a establecer prioridades y determinará la implementación de políticas de control de acceso, aumentando proporcionalmente la seguridad para los datos más críticos de la empresa.

Realizar una clasificación realista de la información que se gestiona en la empresa es uno de los pilares para la correcta elección de las soluciones de seguridad para la empresa, ya que esta clasificación indicará qué sistemas de protección necesita cada tipo de datos y qué usuarios pueden acceder a ellos.

Empresas con mucho recorrido en el campo de seguridad, han recomendado evolucionar sus soluciones de seguridad integrando en un único producto con varias capas de seguridad actuando como si de un tamiz se tratara, encargándose de filtrar posibles amenazas para impedir la infección de los equipos, poder asociar herramientas para que funcionen de forma combinada y coordinada para garantizar la seguridad de los equipos en todos niveles de ejecución, detectando y neutralizando incluso las técnicas de infección más sofisticadas, podría ser una opción acertada para Keralty y blindar más su compañía.

13. Conclusiones

- ✓ Las firmas que más presentaron eventos en el IPS del FW son:
    - HTTP.URI.SQL.Injection
    - MS.RDP.Connection.Brute.force
    - Apache.Strts.2.Jakarta.Multipart.Parse r.Code.Execute
    - Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization

  Estos ataques están asociados a intentos de ejecutar código de manera arbitraria sobre el sitio web de KERALTY (https://www.keralty.com), con fines tales como: robar información de la base de datos del portal, inyectar malware para convertir el portal en una maquina zombie, utilizar el servidor para minar criptomonedas tomar comando y control de la misma, etc.

  Todos estos ataques han sido infructuosos, sin embargo, es posible que en un marco de crecimiento del negocio abriéndose comunicaciones con más países (incluidos los que actualmente están en listas negras) se abre la posibilidad a que se materialice un incidente por un posible ataque exitoso.

- ✓ La guía de buenas prácticas suministrada por el fabricante y aplicada en firewall perimetral de la compañía Keralty disminuyo en un 50 % las vulnerabilidades de la red y en un 28% las vulnerabilidades de los servidores con exposición interna y externa de la compañía, dichas prácticas mantienen el orden, la gestión práctica y la fácil visualización para aplicar

troubleshooting.

- ✓ Se fortalecen los niveles de detección de intrusos, para ello se implementó sistemas de detección al alcance de la empresa dentro del firewall perimetral; estos sistemas fortalecieron con un esquema la segmentación de la red.
- ✓ Con la autorización de la compañía para realizar la investigación y con la aplicación del plan de gestión de vulnerabilidades se utilizaron herramientas técnicamente viables y aprobadas por la empresa, cuyo objetivo fue identificar las vulnerabilidades. Se obtuvieron mejoras en el proceso de gestión de vulnerabilidades análisis de infraestructura y utilización de herramientas apropiadas para gestionar brechas de puertos y servicios abiertos que se encuentran expuestos en seguridad.
- ✓ El sistema actual que soporta la empresa Keralty presenta vulnerabilidades que se evidenciaron de una manera óptima con el uso de la aplicación Nessus y Nmap la cual es muy eficiente en el proceso de análisis de vulnerabilidades y que permite realizar pruebas de intrusión, realizando un escaneo de puertos; permitiendo así la visualización de la infraestructura de red y las deficiencias de la misma.
- ✓ Las vulnerabilidades más relevantes se evidenciaron sobre los servidores que se encuentra en ambiente de preproducción y acorde a las recomendaciones brindadas al director de infraestructura por los creadores de este proyecto se plantea corregirlas antes de salir a producción.
- ✓ Keralty siendo una compañía prestadora de servicios de salud privada y subsidiada atiende recomendaciones y solicita nuestro acompañamiento una vez se corrijan las vulnerabilidades con el fin de brindar un nuevo diagnóstico.

14. Documentación de Referencia

[1] Keralty. (2018). Quienes somos. Disponible en https://www.Keralty.com/usuarios/web/Keralty.

[2] elmundo. (2017). Los hospitales de Reino Unido, en alerta por un ciberataque. Disponible en https://www.elmundo.es/tecnologia/2017/05/12/5915cb15e5fdea24788b4658.html.

[3] Jiménez, Edgar. (2014). Cortafuegos y seguridad en el Internet. Tesis. Instituto politécnico Nacional. México D.F. Disponible en https://tesis.ipn.mx/jspui/bitstream/123456789/15606/1/I.C.E.%2044-14.pdf

[4] Beaver, Kevin. (2017). Firewall best practices. TechTarget. SearchSecurity. Disponible en https://searchsecurity.techtarget.com/tip/Firewall-best-practices

[5] Ferrer, Rodrigo. (s.f.). Metodología recomendada para el análisis de vulnerabilidades. Disponible en http://www.sisteseq.com/files/METODOLOGIA_ANALISIS_DE_VULNERABILIDADES_SISTESEG.doc.

[6] Scribd. (2018). Seguridad informática. Disponible en https://es.scribd.com/document/41519325/Seguridad-Informatica

[7] Instituto Internacional de Seguridad Cibernética. (s.f.). Como hacer análisis de vulnerabilidades informáticas y ventajas del análisis. Disponible en http://www.iicybersecurity.com/analisis-de-vulnerabilidad-informatica.html.

[8] Fortinet. (2018). Disponible en https://www.fortinet.com/

[9] Tenable. (2018). Disponible en https://www.tenable.com/products/nessus.

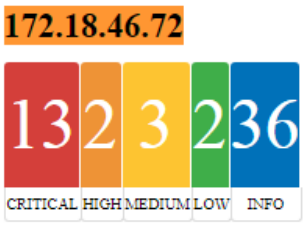
[10] Nmap. (2018). Disponible en https://nmap.org

[11] ATLASSIAN. (2018). Niveles de severidad para problemas de seguridad. Disponible en https://www.atlassian.com/trust/security/security-severity-levels

15. Anexos

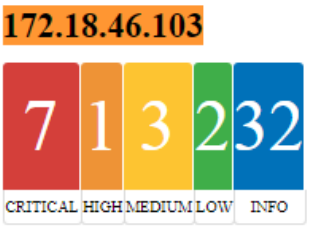
Anexo 1

- 172.18.46.72



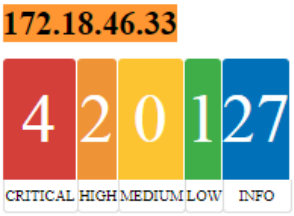
Scan Information
Start time:Mon Oct 22 17:50:27 2018
End time: Mon Oct 22 17:53:48 2018
Host Information
IP: 172.18.46.72
OS:Linux Kernel
Vulnerabilities

- 172.18.46.103



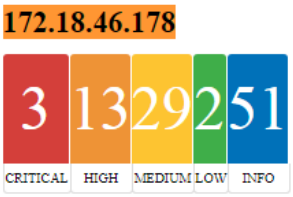
Scan Information
Start time:Mon Oct 22 18:07:33 2018
End time: Mon Oct 22 18:10:30 2018
Host Information
DNS Name:pappwl01.colsanitas.com
IP: 172.18.46.103
OS: Linux Kernel
Vulnerabilities

- 172.18.46.33



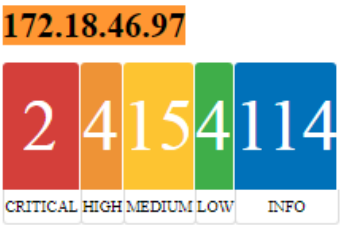
Scan Information
Start time:Mon Oct 22 17:35:54 2018
End time: Mon Oct 22 17:42:47 2018
Host Information
DNS Name:srvvpappwl01.colsanitas.com
IP: 172.18.46.33
Vulnerabilities

- 172.18.46.178



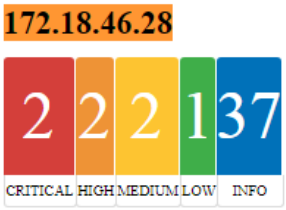
Scan Information
Start time:Mon Oct 22 18:48:20 2018
End time: Mon Oct 22 18:51:16 2018
Host Information
DNS Name: srvvregevenadversos.colsanitas.com
Netbios Name:SRVVREGENADVERS
IP: 172.18.46.178
OS: Microsoft Windows Server 2012 R2 Standard
Vulnerabilities

- 172.18.46.97



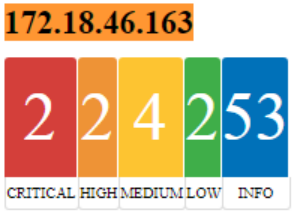
Scan Information
Start time:Mon Oct 22 18:03:26 2018
End time: Mon Oct 22 18:10:48 2018
Host Information
DNS Name:anteo.colsanitas.com
IP: 172.18.46.97
OS: Linux Kernel
Vulnerabilities

- 172.18.46.28



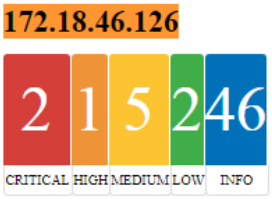
Scan Information
Start time:Mon Oct 22 17:35:16 2018
End time: Mon Oct 22 17:37:13 2018
Host Information
DNS Name:srvvcapacivdj5.colsanitas.com
IP: 172.18.46.28
OS: Linux Kernel
Vulnerabilities

- 172.18.46.163



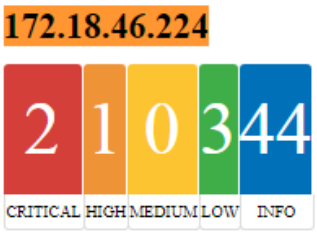
Scan Information
Start time:Mon Oct 22 18:41:42 2018
End time: Mon Oct 22 18:43:47 2018
Host Information
DNS Name:dappj501core.colsanitas.com
IP: 172.18.46.163
OS: Linux Kernel
Vulnerabilities

- 172.18.46.126



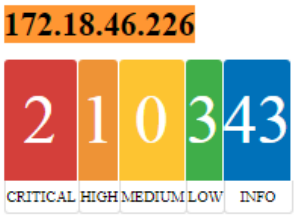
Scan Information
Start time:Mon Oct 22 18:21:53 2018
End time: Mon Oct 22 18:23:54 2018
Host Information
DNS Name: eniopre.colsanitas.com
Netbios Name:AUDISANITAS
IP: 172.18.46.126
OS: Linux Kernel 2.6 on Red Hat Enterprise Linux 5
Vulnerabilities

- 172.18.46.224



Scan Information
Start time:Mon Oct 22 19:10:20 2018
End time: Mon Oct 22 19:12:35 2018
Host Information
DNS Name:srvvebsdb01.colsanitas.com
IP: 172.18.46.224
Vulnerabilities

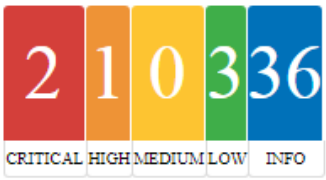
- 172.18.46.226



Scan Information
Start time:Mon Oct 22 19:10:43 2018
End time: Mon Oct 22 19:12:50 2018
Host Information
DNS Name:srvvebsdb01-vip.colsanitas.com
IP: 172.18.46.226
Vulnerabilities

- 172.18.46.229

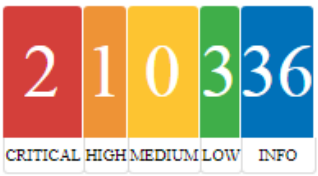
172.18.46.229



Scan Information
Start time:Mon Oct 22 19:12:36 2018
End time: Mon Oct 22 19:15:02 2018
Host Information
DNS Name:preebs-scan.colsanitas.com
IP: 172.18.46.229
Vulnerabilities

- 172.18.46.230

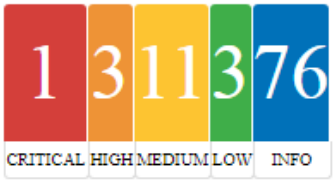
172.18.46.230



Scan Information
Start time:Mon Oct 22 19:12:50 2018
End time: Mon Oct 22 19:15:23 2018
Host Information
DNS Name:preebs-scan.colsanitas.com
IP: 172.18.46.230
Vulnerabilities

- 172.18.46.53

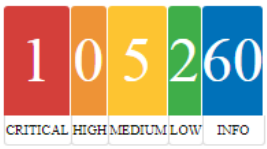
172.18.46.53



Scan Information
Start time:Mon Oct 22 17:43:14 2018
End time: Mon Oct 22 17:47:37 2018
Host Information
IP: 172.18.46.53
OS:AIX 6
Vulnerabilities

- 172.18.46.190

172.18.46.190



Scan Information
Start time:Mon Oct 22 18:53:36 2018
End time: Mon Oct 22 18:56:56 2018
Host Information
DNS Name: srvvsossophiaap.colsanitas.com
Netbios Name:SRVVSOSSOPHIAAP
IP: 172.18.46.190
OS: Microsoft Windows Server 2012 R2 Standard
Vulnerabilities