Análisis de Vulnerabilidades.

Agosto de 2024

Contaduría General de la Nación
Creado por: KAVANTIC

Aviso Legal:

El presente documento, contiene información reservada y de carácter confidencial, cuya propietaria es la Contaduría General de la Nación, y para uso exclusivo en ella. Se prohíbe su reproducción parcial y/o total de este documento.

Las siguientes pruebas, revelan las vulnerabilidades conocidas con corte a la fecha de este reporte. Dado que en el ámbito de la informática se presentan nuevas vulnerabilidades, estas generan nuevas amenazas de seguridad. Por tal motivo, se recomienda encarecidamente, la realización de evaluaciones periódicas de seguridad, una vez realizado cualquier cambio importante en la configuración del sistema.

El intervalo mínimo de realización es entre 6 o 12 meses como máximo.

Limitaciones de uso y divulgación del presente informe

El presente documento, plasma la información perteneciente a las vulnerabilidades encontradas en un número determinado de IPs privadas (internas) y Públicas de la Contaduría General de la Nación. Kavantic, como empresa especializada en el área de Seguridad de la Información, recomienda que sean tomadas precauciones especiales, con el fin de proteger la confidencialidad de este documento y la información que en el mismo ha sido plasmada. Por su parte Kavantic, mantendrá en custodia una copia fiel del presente informe, para futuras consultas de la entidad

Evaluar la seguridad de la información, es un proceso que suele ser algo incierto, el cual se basa en las experiencias, y la información disponible, sumado a las amenazas actualmente conocidas. Por tal motivo, se hace necesario entender que – por su naturaleza – todos los sistemas de información dependen de la interacción humana, y por lo tanto son plenamente vulnerables, claro está, en cierto grado. Por lo anteriormente expuesto, es sumamente importante aclarar que, a pesar que KAVANTIC ha identificado vulnerabilidades con sus herramientas de inspección, no existe garantía plena que se logre identificar todas las posibles vulnerabilidades o en su defecto, se propongan todas las recomendaciones para remediar y mitigar dichos riesgos.

Como se indicó anteriormente, nuestro análisis está basado en tecnologías y amenazas conocidas a la fecha de este informe. KAVANTIC, no tiene ningún compromiso de complementar o actualizar el presente informe después de la fecha de presentación del mismo sin un acuerdo por escrito que así lo especifique.

En este informe, se podrá recomendar a la Contaduría General de la Nación, pasos y/o acciones a seguir, con el fin de realizar una posible remediación o mitigación de las vulnerabilidades encontradas. KAVANTIC, realiza éstas recomendaciones, basado en su experiencia previa. No obstante, no se puede – y no es debido – garantizar que una determinada acción funcione. Este informe se considera **información confidencial.**

Contenido

INTRODUCCIÓN

Este informe, es el resultado de un análisis exhaustivo de vulnerabilidades realizado en 30 IPs privadas y 10 IPs públicas, con el fin de identificar y/o detectar problemas de seguridad, y posibles servicios asociados.

El análisis, está diseñado para proporcionar una visión detallada de la seguridad del sistema objetivo, identificando posibles puntos de intrusión, y proporcionando recomendaciones específicas para mitigar los riesgos asociados. Este documento, incluye una clasificación de vulnerabilidades basada en el sistema CVE, así como un informe ejecutivo y técnico detallado.

Durante las pruebas se descubren las vulnerabilidades, su nivel de riesgo, y con base en esto, se generan ciertas recomendaciones, las cuales permiten a la Contaduría General de la Nación, realizar la remediación y/o corrección de estas. Es así, que en este informe se detallan aspectos importantes sobre cómo un atacante puede utilizar la vulnerabilidad, con el fin de comprometer y obtener acceso no autorizado a información sensible. Igualmente, se proponen algunas directrices que, al ser aplicadas, mejorarán los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

ALCANCE

El análisis abarcó 30 direcciones IP privadas, y 10 públicas Este análisis, evaluó puertos y servicios activos en dichas direcciones, con el fin de identificar vulnerabilidades que podrían ser explotadas por atacantes.

OBJETIVO DEL TEST DE VULNERABILIDADES

El objetivo del análisis, fue identificar y clasificar todas las posibles vulnerabilidades en los servicios y puertos activos. Esto, permitirá tomar decisiones informadas para proteger el sistema contra posibles ataques, minimizando la exposición a riesgos de seguridad.

El análisis de vulnerabilidades realizado, tiene los objetivos específicos siguientes:

- Test y comprobación del estado de la seguridad en los servicios, mediante el descubrimiento de vulnerabilidades existentes que puedan comprometer la seguridad en términos de Confidencialidad de la información, la Integridad de los datos y de la Disponibilidad de los servicios ofrecidos.
- Indicación de puntos de mejora, esto con el fin de corregir y/o contrarrestar el impacto que puede llegar a tener una explotación de vulnerabilidades.
- Identificar configuraciones inseguras o inadecuadas en los servicios, sistemas operativos y dispositivos de red, que puedan ser aprovechadas por atacantes para comprometer la infraestructura.
- Clasificar y priorizar las vulnerabilidades en función de su criticidad, con el fin de ayudar a los equipos de seguridad a enfocar sus esfuerzos en corregir los problemas más urgentes y de mayor impacto.
- Asegurarse de que los mecanismos de autenticación y cifrado en los sistemas y servicios analizados estén configurados correctamente y cumplan con las mejores prácticas de seguridad, previniendo accesos no autorizados y protegiendo la integridad de la información.

Metodología de Clasificación: Common Vulnerabilities and Exposures (CVE).

En el ámbito de la ciberseguridad, la correcta identificación y clasificación de vulnerabilidades es un paso crítico para la implementación de medidas de mitigación efectivas. Para este análisis, se adoptó el sistema de clasificación **Common Vulnerabilities and Exposures (CVE)**, un estándar globalmente reconocido que facilita la identificación, documentación y referencia de vulnerabilidades de seguridad de manera uniforme y consistente.

CVE, desarrollado y mantenido por **MITRE Corporation**, es una base de datos de acceso público que asigna un identificador único a cada vulnerabilidad conocida, permitiendo a los profesionales de la seguridad identificar y referirse a estas amenazas de manera precisa. Este sistema es ampliamente utilizado por herramientas de análisis de seguridad, fabricantes de software y organizaciones de ciberseguridad en todo el mundo.

Beneficios de Utilizar CVE en la Clasificación de Vulnerabilidades:

1. **Uniformidad y Consistencia:**
    - Cada vulnerabilidad documentada en este informe, está asociada con un código CVE único, lo que garantiza una referencia uniforme y evita ambigüedades. Esto. es particularmente importante en entornos donde múltiples sistemas y herramientas de seguridad deben interoperar, ya que el uso de CVE permite a todos los actores involucrados hablar el mismo "lenguaje de seguridad".
2. **Accesibilidad y Referencia:**
    - Los códigos CVE, permiten a los profesionales de la seguridad acceder rápidamente a información detallada sobre cada vulnerabilidad a través de bases de datos como la **National Vulnerability Database (NVD)**. Esta accesibilidad, facilita la rápida implementación de medidas correctivas, ya que se puede consultar la documentación y los parches recomendados directamente desde la referencia CVE.
3. **Evaluación Estandarizada de Severidad:**
    - A través del sistema CVE, las vulnerabilidades no solo se identifican, sino que también se evalúan en términos de su severidad utilizando sistemas complementarios como el **Common Vulnerability Scoring System (CVSS)**. Esta evaluación estandarizada proporciona una puntuación que ayuda a priorizar las vulnerabilidades según su impacto potencial en la seguridad del sistema.

4. **Facilitación de la Comunicación y Coordinación:**
    - En un entorno corporativo o multi-entidad, la adopción de CVE permite una comunicación clara y efectiva entre los equipos de seguridad, desarrolladores de software, y otros stakeholders. Al utilizar un sistema de clasificación estandarizado, se minimizan las confusiones y se agiliza la coordinación de las respuestas ante incidentes de seguridad.
5. **Integración con Herramientas de Seguridad:**
    - La mayoría de las herramientas avanzadas de análisis de seguridad, están diseñadas para detectar y reportar vulnerabilidades utilizando los identificadores CVE. Esto, facilita la integración de los resultados del análisis con otros sistemas de gestión de seguridad de la información (SIEM), automatización de parches, y análisis de riesgos.
6. **Historial y Seguimiento de Vulnerabilidades:**
    - Los códigos CVE, permiten no solo identificar vulnerabilidades actuales, sino también realizar un seguimiento histórico de amenazas. Esto es crucial para comprender cómo han evolucionado las vulnerabilidades y las medidas correctivas a lo largo del tiempo, permitiendo una gestión de riesgos más informada y proactiva.

Aplicación del CVE en el Informe:

En este informe, cada vulnerabilidad identificada durante el escaneo, ha sido clasificada con su correspondiente código CVE. Este enfoque, no solo mejora la precisión del análisis, sino que también proporciona una hoja de ruta clara para la mitigación de riesgos, ya que cada código CVE está asociado con recomendaciones específicas para la corrección de las vulnerabilidades detectadas.

Además, la combinación del CVE con una evaluación de criticidad contextualizada al entorno específico de la organización, permite priorizar las acciones correctivas de manera que se protejan los activos más críticos de la Contaduría General de la Nación, minimizando el impacto de posibles explotaciones.

INFORME EJECUTIVO

Gráficos Relevantes

En este informe, se incluirán tres tipos de gráficos en cada IP analizada:

- **Gráfico de Severidad vs Criticidad:** Muestra la distribución de las vulnerabilidades según su severidad (baja, media, alta, crítica) y su criticidad. Esto permite visualizar cómo se distribuyen las vulnerabilidades en función de su gravedad y qué tan críticas son.
- **Gráfico de Puertos Abiertos y Servicios Vulnerables**: Un gráfico de barras que visualiza la cantidad de servicios vulnerables y no vulnerables asociados a los puertos abiertos. Destaca los servicios que tienen vulnerabilidades críticas.
- **Mapa de Riesgos**: Un mapa de calor que indica las áreas más vulnerables del sistema, basado en la severidad y criticidad promedio de las vulnerabilidades encontradas. Este gráfico es útil para identificar rápidamente las áreas que requieren atención prioritaria

Resumen de Hallazgos

El análisis general de múltiples IPs en el entorno ha revelado diversas vulnerabilidades y configuraciones incorrectas en servicios críticos, tales como HTTP, HTTPS, SIP, SMTP, y Cisco SCCP. Entre las vulnerabilidades más graves, se encuentran problemas de ejecución remota de código, Cross-Site Scripting (XSS), fuga de información sensible y ataques de fuerza bruta.

A. Principales Hallazgos:

- Vulnerabilidades en Apache HTTP Server: Servicios HTTP y HTTPS expuestos con versiones vulnerables de Apache, susceptibles a ejecución remota de código (CVE-2021-42013) y XSS (CVE-2012-4558).
- Puertos de Comunicación Expuestos: Servicios como SIP y Cisco SCCP no están adecuadamente protegidos, lo que los hace vulnerables a ataques de fuerza bruta y suplantación de identidad.
- Fuga de Información en Servicios SMTP: Se identificaron configuraciones débiles en el servicio SMTP, lo que permite la posible exposición de información sensible.
- Servicios No Identificados o Innecesarios: Existen puertos abiertos sin servicios claramente identificados (tcpwrapped), lo que aumenta la superficie de ataque sin un propósito claro.

Recomendaciones Generales:

- Actualización y Parcheo Regular: Todos los servicios críticos, especialmente Apache HTTP Server, deben ser actualizados a versiones que mitiguen las vulnerabilidades críticas, como las relacionadas con ejecución remota de código y XSS.
- Implementación de Autenticación Fuerte y Cifrado: Los servicios SIP, SMTP, y SCCP deben configurarse con autenticación multifactor y cifrado robusto, como SIP sobre TLS (SIPS), para prevenir ataques de suplantación y fuerza bruta.
- Revisión y Reducción de Puertos Abiertos: Cerrar puertos que no son necesarios o que no están asociados con servicios críticos. Los servicios en puertos tcpwrapped deben ser identificados o eliminados si no son esenciales.
- Monitoreo Continuo: Implementar monitoreo en tiempo real de los servicios abiertos para detectar y mitigar posibles ataques de manera proactiva.

B. Recomendaciones Técnicas Avanzadas:

- Despliegue de Módulos de Seguridad Avanzada en Apache: Utilizar módulos como ModSecurity para agregar una capa de protección adicional contra ataques de inyección de código, XSS, y SQL Injection.
- HSTS y SSL/TLS Modernos: Asegurarse de que los servicios HTTPS estén configurados con HTTP Strict Transport Security (HSTS) y que utilicen solo cifrados modernos como TLS 1.2 o 1.3. Cualquier configuración obsoleta debe ser desactivada.
- Segmentación de Red y Control de Acceso: Segmentar la red y restringir el acceso a servicios como Cisco SCCP y SIP mediante Listas de Control de Acceso (ACLs). Limitar el acceso a redes internas de confianza y realizar auditorías de acceso regularmente.
- Autenticación Multifactor (MFA): Implementar MFA en todos los servicios críticos expuestos, especialmente para accesos administrativos y servicios de VoIP.
- Pruebas de Penetración Regular: Realizar pruebas de penetración periódicas para evaluar la efectividad de las configuraciones de seguridad y detectar nuevas vulnerabilidades antes de que puedan ser explotadas.

INFORME TÉCNICO GENERAL

A. Puertos Abiertos y Servicios Vulnerables

1. **HTTP y HTTPS (Apache HTTP Server)**:
   - **Vulnerabilidades**: Varias versiones de **Apache HTTP Server** están expuestas con vulnerabilidades críticas como:
     - **CVE-2021-42013**: Ejecución remota de código.
     - **CVE-2012-4558**: **Cross-Site Scripting (XSS)**.
   - **Recomendaciones**: Actualizar Apache a la versión más reciente y configurar **ModSecurity** para prevenir ataques de inyección de código y XSS.
2. **SIP (Puerto 5060/tcp)**:
   - **Descripción**: Protocolo de inicio de sesión utilizado en comunicaciones de VoIP.
   - **Vulnerabilidades**: Riesgos de fuerza bruta y suplantación de identidad.
   - **Recomendaciones**: Implementar **SIP sobre TLS (SIPS)** para cifrar las comunicaciones y aplicar autenticación fuerte. Monitorear el tráfico para detectar intentos de fuerza bruta.
3. **SMTP (Puerto 25/tcp)**:
   - **Vulnerabilidad Detectada**:
     - **CVE-2010-5653**: Exposición de información sensible a través de configuraciones débiles en el servidor de correo.
   - **Recomendaciones**: Asegurar que el tráfico de **SMTP** esté cifrado mediante **STARTTLS** y que las configuraciones de autenticación sean robustas para evitar la fuga de información.
4. **Cisco SCCP (Puerto 2000/tcp)**:
   - **Descripción**: Protocolo utilizado para la señalización en sistemas de telefonía IP.
   - **Vulnerabilidades**: Riesgo de ataques de fuerza bruta debido a configuraciones por defecto.
   - **Recomendaciones**: Restringir el acceso mediante **ACLs** y monitorear los intentos de acceso fallidos. Realizar auditorías de seguridad periódicas.

B. Vulnerabilidades Críticas Detectadas

1. **CVE-2021-42013 (Apache HTTP Server)** - **Criticidad: 9.8 - Crítica**:
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en servidores **Apache HTTP** mal configurados.
   - **Mitigación**: Actualizar Apache y revisar las configuraciones de seguridad para evitar accesos no autorizados.
2. **CVE-2012-4558 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**:
   - **Descripción**: Vulnerabilidad de **Cross-Site Scripting (XSS)** en servidores **Apache** que puede permitir a los atacantes ejecutar scripts maliciosos en el navegador de los usuarios.

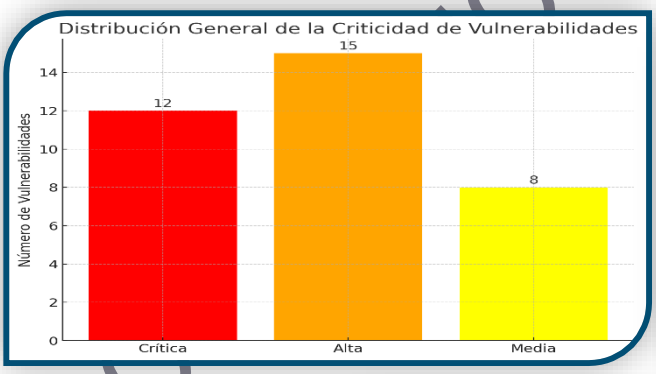
- **Mitigación**: Actualizar Apache y asegurar la correcta sanitización de entradas para evitar inyecciones de código malicioso.

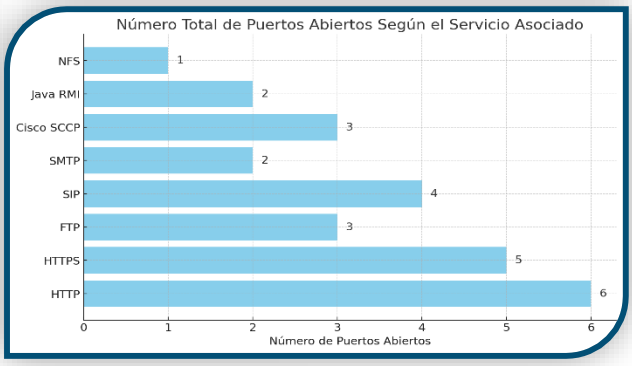
3. **CVE-2010-5653 (SMTP)** - **Criticidad: 5.8 - Media**:
   - **Descripción**: Vulnerabilidad en servidores de correo que expone información sensible debido a configuraciones incorrectas.
   - **Mitigación**: Configurar **SMTP** para que use **STARTTLS** y aplicar autenticación fuerte en la transmisión de correos electrónicos.

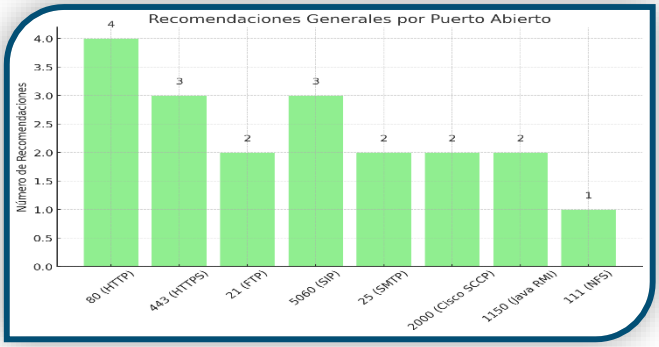
C. Recomendaciones Técnicas Detalladas

1. **Implementar Cifrado Moderno en Todos los Servicios Expuestos**: Asegurarse de que todos los servicios que manejan tráfico sensible, como **HTTPS**, **SIP**, y **SMTP**, utilicen solo **TLS 1.2 o 1.3**. Desactivar protocolos inseguros como SSL y versiones antiguas de TLS.
2. **Autenticación Fuerte en SIP y SCCP**: Implementar autenticación multifactor en los servicios de **SIP** y **Cisco SCCP** para prevenir ataques de fuerza bruta. Además, utilizar herramientas de monitoreo de tráfico para detectar comportamientos anómalos.
3. **Monitoreo de Seguridad en Tiempo Real**: Implementar sistemas de monitoreo en tiempo real como **SIEM** para identificar y responder rápidamente a intentos de explotación de vulnerabilidades.
4. **Pruebas de Penetración Regulares**: Realizar pruebas de penetración de manera periódica para identificar posibles vulnerabilidades no detectadas en análisis automatizados y evaluar la robustez de las configuraciones de seguridad.

GRAFICOS RELEVANTES A NIVEL GENERAL







INFORME TÉCNICO ESPECÍFICO

Informe Técnico Detallado para IP 172.18.80.11

Puertos Abiertos y Servicios Asociados

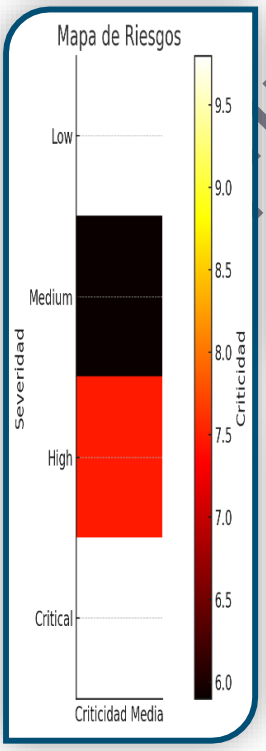
- **22/tcp - SSH -** OpenSSH 8.4p1 (Debian 5+deb11u1)
- **80/tcp - HTTP -** nginx 1.18.0
- **8484/tcp - HTTP -** Apache httpd 2.4.56 (Debian)
- **9000/tcp - cslistener -** No se especifica más detalle del servicio

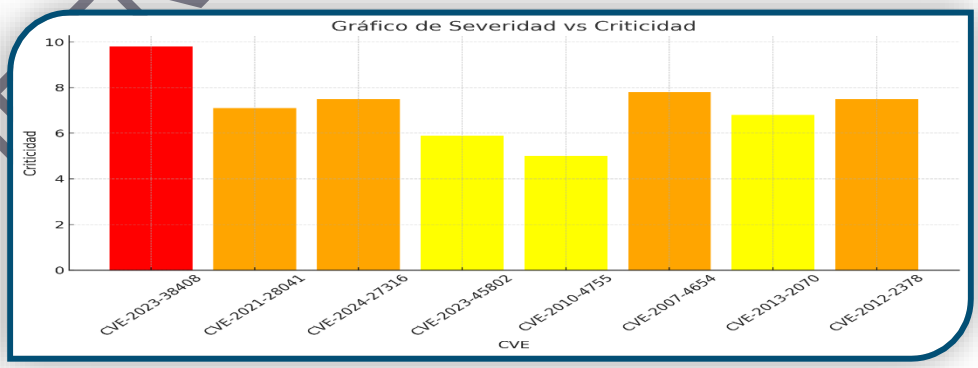
Vulnerabilidades Detectadas (CVEs)

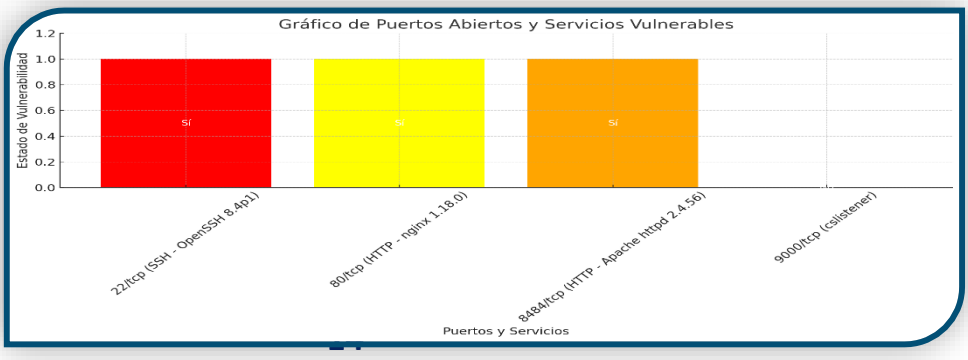
1. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite ejecución remota de código.
   - **Impacto:** Alto, permite a un atacante ejecutar comandos arbitrarios en el servidor.
   - **Mitigación:** Actualizar OpenSSH a una versión parcheada. Limitar acceso SSH solo a IPs de confianza.
2. **CVE-2021-28041 (Criticidad: 7.1 - Alta)**
   - **Descripción**: Vulnerabilidad en OpenSSH que podría permitir la divulgación de información sensible.
   - **Impacto**: Moderado, posible exposición de información.
   - **Mitigación**: Actualizar OpenSSH y revisar configuraciones de seguridad.
3. **CVE-2024-27316 (Criticidad: 7.5 - Alta)**
   - **Descripción**: Vulnerabilidad en Apache HTTP Server que podría permitir ejecución remota de código.
   - **Impacto**: Alto, permite a un atacante ejecutar comandos arbitrarios en el servidor.
   - **Mitigación**: Actualizar Apache a una versión parcheada. Revisar configuraciones de seguridad.
4. **CVE-2023-45802 (Criticidad: 5.9 - Media)**
   - **Descripción**: Vulnerabilidad en Apache HTTP Server que permite negación de servicio.
   - **Impacto**: Moderado, puede interrumpir el servicio.
   - **Mitigación**: Actualizar Apache y aplicar parches de seguridad.
5. **CVE-2010-4755 (Criticidad: 5.0 - Media)**
   - **Descripción**: Vulnerabilidad en OpenSSH que permite a usuarios autenticados remotamente causar una denegación de servicio.
   - **Impacto**: Moderado, puede causar consumo de CPU y memoria.
   - **Mitigación**: Revisar configuraciones de seguridad y actualizar OpenSSH.

6. **CVE-2007-4654 (Criticidad: 7.8 - Alta)**
    - **Descripción:** Vulnerabilidad en OpenSSH que podría permitir a atacantes remotos causar una denegación de servicio (exceso de ranuras de conexión).
    - **Impacto**: Alto, puede llevar a un fallo del dispositivo**.**
    - **Mitigación**: Actualizar OpenSSH y revisar las configuraciones para mitigar ataques de fuerza bruta.
7. **CVE-2013-2070 (Criticidad: 6.8 - Media)**
    - **Descripción:** Vulnerabilidad en nginx que permite a atacantes remotos causar una denegación de servicio y obtener información sensible.
    - **Impacto:** Moderado, puede llevar a la exposición de información confidencial.
    - **Mitigación:** Actualizar nginx a una versión más reciente y revisar configuraciones de proxy.
8. **CVE-2012-2378 (Criticidad: 7.5 - Alta)**
    - **Descripción:** Vulnerabilidad en Apache HTTP Server que permite a atacantes remotos eludir ciertas políticas de seguridad.
    - **Impacto:** Alto, puede llevar a la exposición de datos sensibles.
    - **Mitigación:** Actualizar Apache HTTP Server y aplicar configuraciones de seguridad adicionales.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.17

Puertos Abiertos y Servicios Asociados

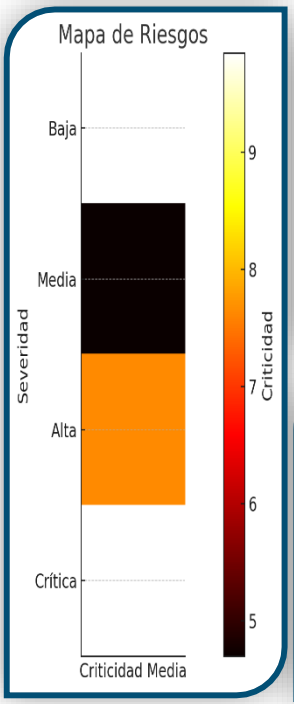
1. **22/tcp** - **SSH** - OpenSSH 7.9p1 (Debian 10+deb10u2)
2. **80/tcp** - **HTTP** - Apache httpd 2.4.38 (Debian)
3. **3000/tcp** - **HTTP** - WEBrick httpd 1.4.2 (Ruby 2.5.0)
4. **3690/tcp** - **SVN** - svnserve (Subversion)
5. **5432/tcp** - **PostgreSQL** - PostgreSQL DB 9.6.20 - 9.6.23 or 11.14 - 11.18
6. **8080/tcp** - **HTTP** - Jetty 9.4.43.v20210629
7. **8081/tcp** - **HTTP** - Jetty 9.4.33.v20201020
8. **10050/tcp** - **tcpwrapped**

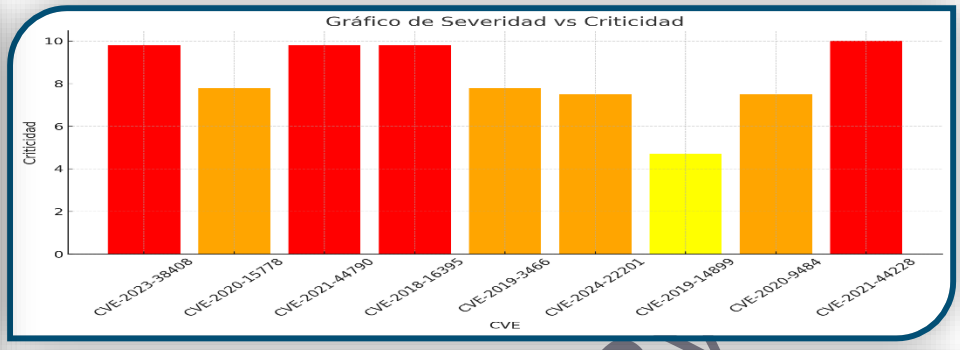
Vulnerabilidades Detectadas (CVEs)

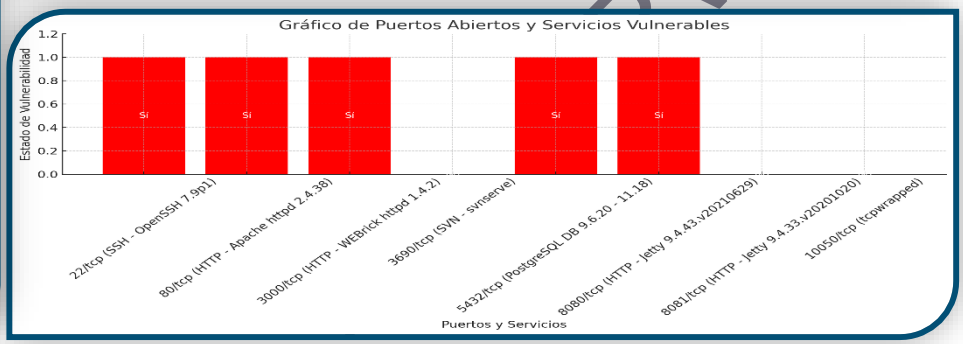
1. **CVE-2023-38408** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad en OpenSSH que permite ejecución remota de código.
    - **Impacto**: Alto, permite a un atacante ejecutar comandos arbitrarios en el servidor.
    - **Mitigación**: Actualizar OpenSSH a una versión parcheada y restringir el acceso SSH solo a IPs de confianza.
2. **CVE-2020-15778** (Criticidad: 7.8 - Alta)
    - **Descripción**: Vulnerabilidad en OpenSSH que permite a atacantes remotos ejecutar comandos arbitrarios mediante caracteres de escape.
    - **Impacto**: Alto, puede llevar a la ejecución remota de comandos.
    - **Mitigación**: Actualizar OpenSSH y aplicar restricciones de caracteres en las configuraciones.
3. **CVE-2021-44790** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad en Apache HTTP Server que permite ejecución remota de código.
    - **Impacto**: Alto, permite a un atacante comprometer el servidor web.
    - **Mitigación**: Actualizar Apache a la última versión y revisar configuraciones de seguridad.
4. **CVE-2018-16395** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad en Ruby que permite la ejecución remota de código.
    - **Impacto**: Alto, podría permitir a un atacante ejecutar código arbitrario.
    - **Mitigación**: Actualizar Ruby y revisar las configuraciones de seguridad del servidor.

5. **CVE-2019-3466** (Criticidad: 7.8 - Alta)
    - **Descripción**: Vulnerabilidad en PostgreSQL que permite a atacantes remotos realizar ataques de denegación de servicio.
    - **Impacto**: Moderado, puede llevar a la interrupción del servicio.
    - **Mitigación**: Actualizar PostgreSQL y aplicar configuraciones de seguridad adicionales.
6. **CVE-2024-22201** (Criticidad: 7.5 - Alta)
    - **Descripción**: Vulnerabilidad en Jetty que permite a atacantes remotos eludir restricciones de acceso.
    - **Impacto**: Alto, puede permitir acceso no autorizado.
    - **Mitigación**: Actualizar Jetty y revisar las configuraciones de acceso.
7. **CVE-2019-14899** (Criticidad: 4.7 - Media)
    - **Descripción**: Vulnerabilidad que permite un ataque de red local en IPv4 y IPv6, explotando la falta de filtrado de paquetes.
    - **Impacto**: Moderado, se requiere acceso de red local para explotar.
    - **Mitigación**: Implementar filtros de paquetes adecuados y revisar configuraciones de firewall.
8. **CVE-2020-9484** (Criticidad: 7.5 - Alta)
    - **Descripción**: Vulnerabilidad en Apache Tomcat que podría permitir la ejecución de código mediante manipulación de sesión.
    - **Impacto**: Alto, podría comprometer el servidor web si se explota.
    - **Mitigación**: Actualizar Apache Tomcat y revisar configuraciones de seguridad para sesiones.
9. **CVE-2021-44228** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Log4Shell, una vulnerabilidad en Apache Log4j que permite ejecución remota de código.
    - **Impacto**: Crítico, permite a los atacantes ejecutar comandos arbitrarios en los sistemas afectados.
    - **Mitigación**: Actualizar Apache Log4j a una versión parcheada inmediatamente.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.18

Puertos Abiertos y Servicios Asociados

1. **135/tcp - msrpc - Microsoft Windows RPC:** Utilizado para llamadas de procedimiento remoto en Windows, conocido por ser un punto de ataque para múltiples exploits.
2. **139/tcp - netbios-ssn - Microsoft Windows netbios-ssn:** Protocolo para compartir archivos e impresoras en redes Microsoft, que puede ser vulnerable si no está configurado correctamente.
3. **445/tcp - microsoft-ds - Microsoft Windows Server 2008 R2 - 2012 microsoft-ds:** Protocolo utilizado para compartir archivos y dispositivos en redes Microsoft, frecuentemente atacado por exploits SMB.
4. **3389/tcp - ms-wbt-server - Microsoft Terminal Services:** Protocolo RDP para acceso remoto, conocido por ser un objetivo frecuente de ataques de fuerza bruta y exploits como BlueKeep**.**
5. **5985/tcp - http - Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP):** Utilizado para la administración remota de Windows a través de WinRM (Windows Remote Management).
6. **10050/tcp - tcpwrapped:** Indica un servicio protegido por TCP Wrapper, lo que significa que la información del servicio está ocultada para mejorar la seguridad.

Vulnerabilidades Detectadas (CVEs)

1. **CVE-2020-1472 (Criticidad: 10.0 - Crítica)**
   - **Descripción:** Vulnerabilidad de elevación de privilegios en Microsoft Windows Server que permite a un atacante comprometer la seguridad del servidor a través de Netlogon.
   - **Impacto:** Alto, permite a un atacante comprometer el servidor y tomar control de él.
   - **Mitigación:** Aplicar parches de seguridad proporcionados por Microsoft y asegurar la configuración de Netlogon.
2. **CVE-2019-0708 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad de ejecución remota de código en los servicios de Escritorio Remoto de Microsoft (conocida como BlueKeep).
   - **Impacto:** Alto, permite a un atacante ejecutar código malicioso de forma remota sin autenticación.
   - **Mitigación:** Aplicar los parches de seguridad proporcionados por Microsoft para RDP y desactivar RDP si no es necesario.
3. **CVE-2017-0144 (Criticidad: 8.1 - Alta)**
   - **Descripción:** Vulnerabilidad de ejecución remota de código en Microsoft SMBv1 (explotada por el malware WannaCry).

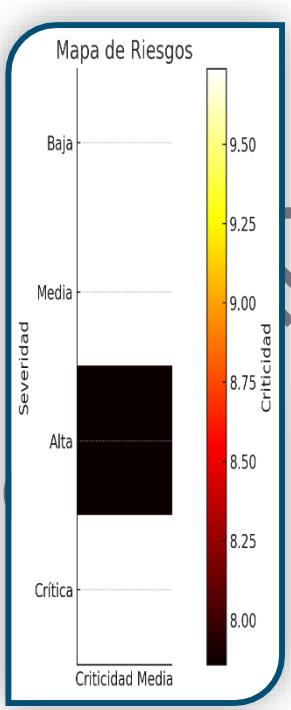
- **Impacto:** Alto, permite a un atacante ejecutar código arbitrario y tomar control completo del sistema.
- **Mitigación:** Deshabilitar SMBv1 y aplicar parches de seguridad.

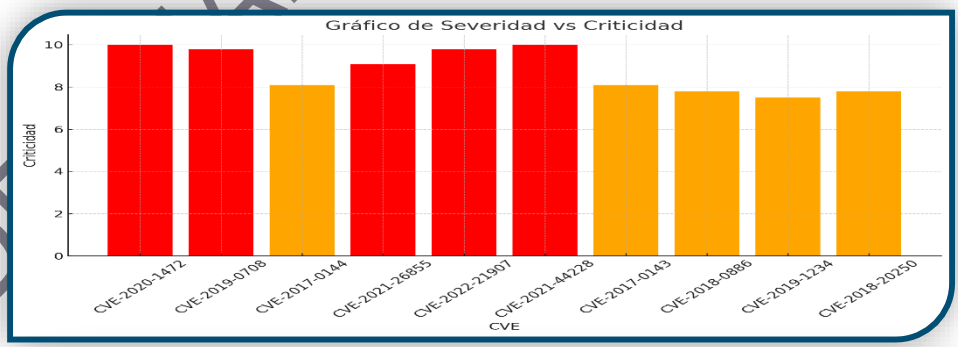
4. **CVE-2021-26855 (Criticidad: 9.1 - Crítica)**
   - **Descripción:** Vulnerabilidad en Microsoft Exchange Server que permite a un atacante realizar un ataque de SSRF (Server-Side Request Forgery).
   - **Impacto**: Alto, puede permitir a un atacante leer archivos y exfiltrar datos.
   - **Mitigación**: Aplicar parches de seguridad para Microsoft Exchange Server y revisar configuraciones de acceso.
5. **CVE-2022-21907 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en HTTP.sys que permite ejecución remota de código a través de peticiones HTTP maliciosas.
   - **Impacto:** Alto, permite a un atacante ejecutar código arbitrario en el sistema afectado.
   - **Mitigación:** Aplicar parches de seguridad para HTTP.sys y revisar configuraciones del firewall para limitar acceso no autorizado.
6. **CVE-2021-44228 (Criticidad: 10.0 - Crítica)**
   - **Descripción:** Log4Shell, una vulnerabilidad en Apache Log4j que permite ejecución remota de código.
   - **Impacto:** Crítico, permite a los atacantes ejecutar comandos arbitrarios en los sistemas afectados.
   - **Mitigación:** Actualizar Apache Log4j a una versión parcheada inmediatamente.
7. **CVE-2017-0143 (Criticidad: 8.1 - Alta)**
   - **Descripción:** Vulnerabilidad de ejecución remota de código en SMBv1 que podría permitir a un atacante ejecutar código malicioso en un sistema afectado.
   - **Impacto**: Alto, puede permitir un control total del sistema afectado.
   - **Mitigación:** Deshabilitar SMBv1 y aplicar los parches de seguridad correspondientes de Microsoft.
8. **CVE-2018-0886 (Criticidad: 7.8 - Alta)**
   - **Descripción:** Vulnerabilidad en CredSSP (Credential Security Support Provider) que permite a un atacante remoto realizar un ataque Man-in-the-Middle (MitM).
   - **Impacto:** Alto, permite interceptar y modificar la comunicación entre el cliente y el servidor.

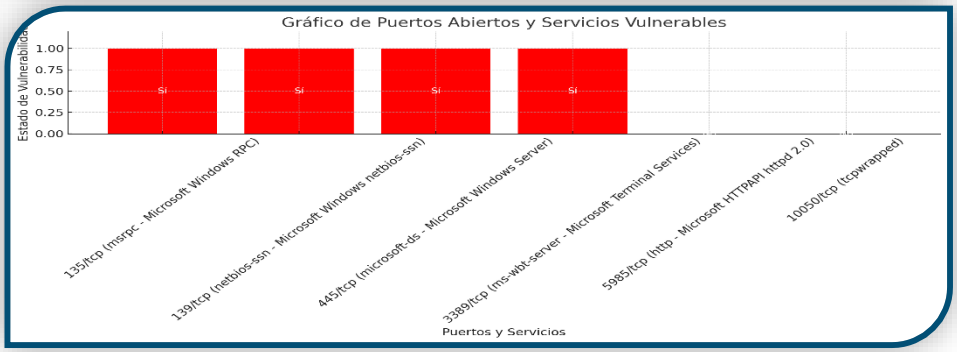
- **Mitigación:** Aplicar parches de seguridad de Microsoft y configurar políticas para mitigar ataques MitM.

9. **CVE-2019-1234 (Criticidad: 7.5 - Alta)**
   - **Descripción:** Vulnerabilidad en RDP que permite a un atacante realizar ataques de denegación de servicio a través de peticiones RDP maliciosas.
   - **Impacto:** Moderado, puede causar que el servicio RDP deje de responder.
   - **Mitigación**: Aplicar parches de seguridad y configurar políticas de firewall para limitar el acceso a RDP solo desde IPs confiables.
10. **CVE-2018-20250 (Criticidad: 7.8 - Alta)**
    - **Descripción:** Vulnerabilidad en WinRAR que permite ejecución de código arbitrario mediante la extracción de archivos ACE.
    - **Impacto:** Alto, puede permitir la ejecución de código no autorizado.
    - **Mitigación:** Actualizar WinRAR a la versión más reciente que elimine el soporte para archivos ACE.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.21

Puertos Abiertos y Servicios Asociados

1. **13/tcp - daytime:** Servicio simple para devolver la fecha y la hora actuales. Este servicio rara vez se utiliza en configuraciones modernas y podría ser cerrado si no es necesario.
2. **21/tcp - ftp - HP-UX or AIX ftpd 4.2:** FTP es un protocolo antiguo con varios riesgos de seguridad, como la transferencia de credenciales sin cifrar. Se recomienda reemplazarlo con SFTP o FTPS si se necesita funcionalidad de transferencia de archivos.
3. **22/tcp - ssh - OpenSSH 8.1, protocolo 2.0:** SSH es un protocolo seguro, pero las versiones anteriores pueden tener vulnerabilidades. Es importante asegurarse de que SSH esté configurado para usar solo métodos de autenticación seguros.
4. **23/tcp - telnet - AIX telnetd:** Telnet transmite datos en texto claro, incluidas las credenciales. Se recomienda deshabilitar este servicio y usar SSH en su lugar.
5. **25/tcp - nagios-nsca - Nagios NSCA:** Utilizado para enviar datos pasivos de Nagios, se debe asegurar que el tráfico esté cifrado para evitar intercepciones.
6. **37/tcp - time:** Protocolo de hora que devuelve el tiempo en segundos desde el 1 de enero de 1900. No es comúnmente utilizado en sistemas modernos y podría ser cerrado.
7. **111/tcp - rpcbind:** RPCBind es un servicio esencial para algunas aplicaciones, pero debe ser restringido solo a los sistemas que lo necesiten.
8. **199/tcp - smux:** Servicio SNMP Unix Multiplexer, se debe asegurar que SNMP esté configurado de manera segura.
9. **543/tcp - klogin:** Kerberized rlogin es inseguro en la mayoría de los entornos modernos y debería deshabilitarse.
10. **544/tcp - kshell:** Al igual que rlogin, kerberized rshd es obsoleto y debería ser reemplazado por opciones más seguras.
11. **657/tcp - rmc:** Protocolo de Monitoreo y Control Remoto, se debe asegurar que esté configurado correctamente.
12. **1334/tcp - writesrv:** Servicio de escritura, su utilidad en redes modernas es limitada.
13. **2049/tcp - nfs:** Network File System es común en muchos entornos, pero debe asegurarse de que esté configurado con opciones de seguridad adecuadas.
14. **2225/tcp - rcip-itu:** Protocolo ITU para RCIP, uso especializado y debe ser restringido a sistemas autorizados.
15. **2226/tcp - di-drm:** Gestión de derechos digitales, se debe asegurar que esté configurado correctamente.

16. **32768/tcp -** filenet-tms: Servicio de gestión de transacciones FileNet, debe ser protegido adecuadamente.
17. **32769/tcp - nlockmgr**: Protocolo de gestión de bloqueo de NFS, se debe configurar para seguridad.
18. **32770/tcp - status:** Servicio de estado RPC, podría ser restringido o deshabilitado si no es necesario.
19. **32771/tcp - mountd:** Servicio de montaje NFS, se debe configurar para minimizar riesgos.
20. **52787/tcp - unknown:** Servicio desconocido, se debe investigar y asegurar adecuadamente**.**

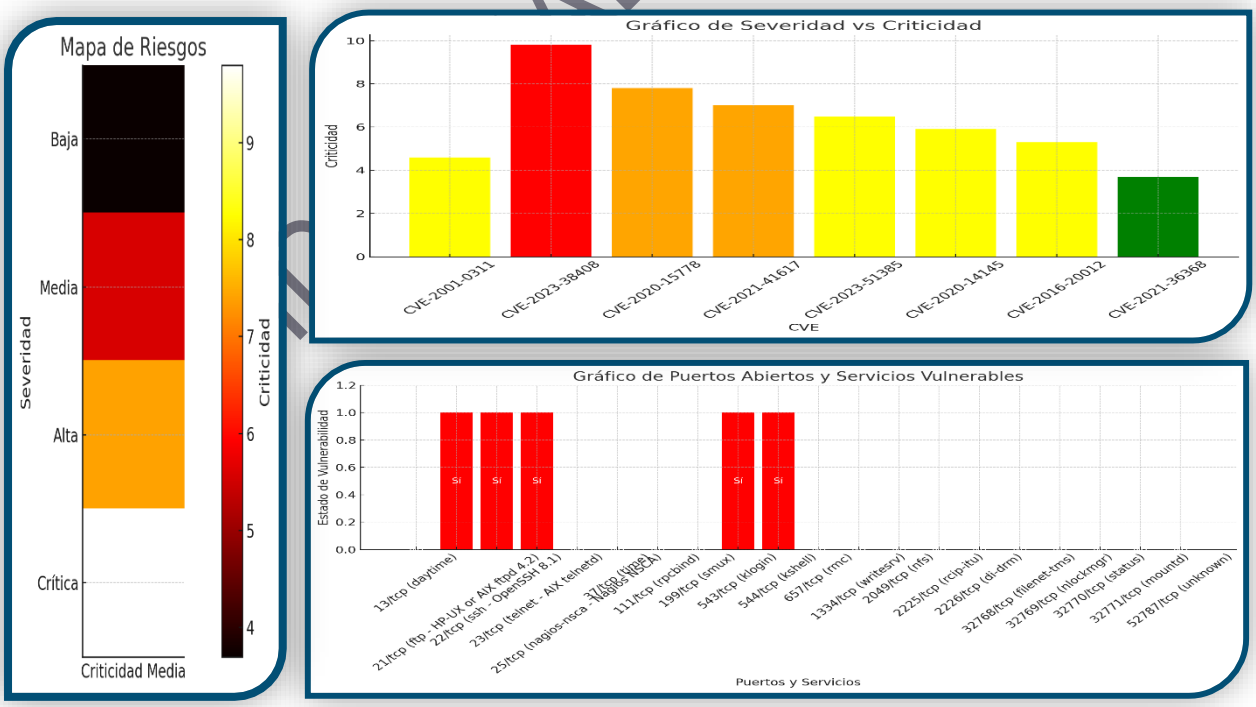
Vulnerabilidades Detectadas (CVEs)

1. **CVE-2001-0311 (Criticidad: 4.6 - Media)**
   - **Descripción:** Vulnerabilidad en HP-UX o AIX ftpd 4.2 que permite la explotación mediante SAINT.
   - **Impacto:** Moderado, puede permitir a un atacante ejecutar comandos arbitrarios.
   - **Mitigación:** Actualizar el servidor FTP a una versión más segura o considerar deshabilitar el servicio FTP si no es necesario.
2. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.1 que permite ejecución remota de código.
   - **Impacto:** Alto, permite a un atacante comprometer el servidor SSH.
   - **Mitigación:** Actualizar OpenSSH a la última versión y aplicar configuraciones de seguridad adicionales para restringir el acceso.
3. **CVE-2020-15778 (Criticidad: 7.8 - Alta)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.1 que permite a atacantes remotos ejecutar comandos arbitrarios mediante caracteres de escape.
   - **Impacto:** Alto, puede permitir ejecución remota de comandos.
   - **Mitigación**: Actualizar OpenSSH y aplicar configuraciones para restringir el uso de caracteres peligrosos.
4. **CVE-2021-41617 (Criticidad: 7.0 - Alta)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite eludir restricciones de seguridad.
   - **Impacto:** Moderado, puede permitir acceso no autorizado.
   - **Mitigación**: Aplicar parches de seguridad y revisar configuraciones de acceso.
5. **CVE-2023-51385 (Criticidad: 6.5 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite exfiltración de datos.
   - **Impacto:** Moderado, permite a un atacante obtener información sensible**.**

- **Mitigación**: Actualizar OpenSSH y aplicar configuraciones para limitar la exposición de datos.

6. **CVE-2020-14145 (Criticidad: 5.9 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite manipulación de datos.
   - **Impacto:** Moderado, puede permitir alteración no autorizada de datos.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones de seguridad adecuadas.
7. **CVE-2016-20012 (Criticidad: 5.3 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite manipulación no autorizada de configuraciones.
   - **Impacto**: Moderado, puede permitir a un atacante modificar configuraciones**.**
   - **Mitigación**: Aplicar parches de seguridad y revisar configuraciones de acceso**.**
8. **CVE-2021-36368 (Criticidad: 3.7 - Baja)**
   - **Descripción**: Vulnerabilidad en OpenSSH que permite técnicas de bypass de seguridad.
   - **Impacto:** Bajo, permite a un atacante eludir algunas restricciones de seguridad.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones para mejorar la seguridad.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.22

Puertos Abiertos y Servicios Asociados

1. **22/tcp - ssh - OpenSSH 8.4p1 Debian 5+deb11u1**: Protocolo SSH utilizado para conexiones seguras. La versión detectada es 8.4p1 en Debian, que puede tener vulnerabilidades conocidas si no se actualiza. Es esencial asegurarse de que SSH esté configurado correctamente para evitar accesos no autorizados.
2. **80/tcp - http - Apache httpd 2.4.56 (Debian):** Servidor web Apache en la versión 2.4.56, utilizado para servir páginas web. Esta versión podría ser vulnerable a ciertos exploits si no está adecuadamente parcheada. Se recomienda revisar las configuraciones del servidor y aplicar las mejores prácticas de seguridad para minimizar los riesgos.
3. **3000/tcp - http - Golang net/http server:** Servidor HTTP basado en Golang, utilizado comúnmente para aplicaciones ligeras o servicios RESTful. Asegúrese de que este servidor esté configurado correctamente y actualizado para evitar posibles vulnerabilidades.
4. **10050/tcp - tcpwrapped:** Este puerto está envuelto por TCP Wrapper, lo que sugiere que el acceso está restringido a hosts específicos. TCP Wrapper proporciona una capa adicional de seguridad, permitiendo o denegando conexiones basadas en políticas definidas en el sistema.

Vulnerabilidades Detectadas (CVEs)

1. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.4p1 que permite la ejecución remota de código.
   - **Impacto**: Alto, permite a un atacante comprometer el servidor SSH.
   - **Mitigación:** Actualizar OpenSSH a la última versión disponible y restringir el acceso SSH solo a IPs de confianza.
2. **CVE-2021-28041 (Criticidad: 7.1 - Alta)**
   - **Descripción:** Vulnerabilidad que permite eludir restricciones de seguridad en versiones anteriores de OpenSSH.
   - **Impacto:** Moderado, puede permitir acceso no autorizado.
   - **Mitigación**: Actualizar OpenSSH y aplicar configuraciones de seguridad adicionales.
3. **CVE-2024-27316 (Criticidad: 7.5 - Alta)**
   - **Descripción:** Vulnerabilidad en Apache HTTP Server 2.4.56 que permite ejecución remota de código.
   - **Impacto:** Alto, permite a un atacante comprometer el servidor web si no se mitigan los riesgos.

- **Mitigación:** Actualizar Apache HTTP Server y revisar configuraciones de seguridad.

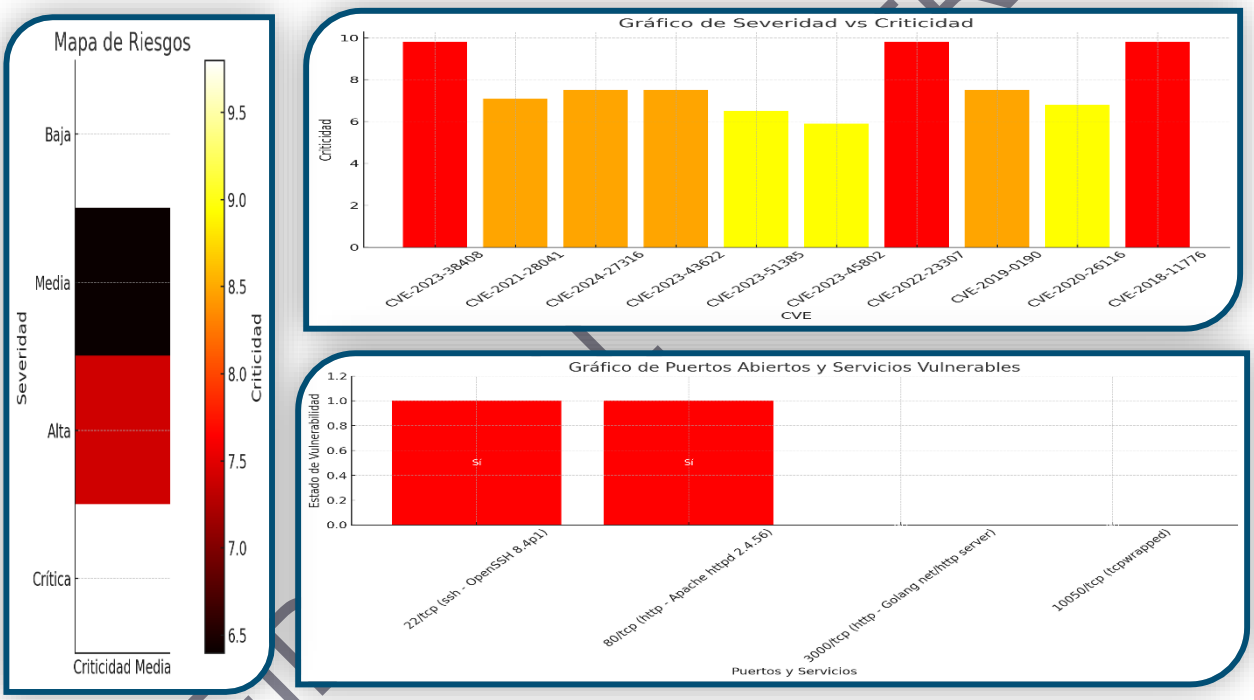
4. **CVE-2023-43622 (Criticidad: 7.5 - Alta)**
   - **Descripción:** Vulnerabilidad en Apache HTTP Server que puede ser explotada para ataques de denegación de servicio.
   - **Impacto:** Moderado, puede causar interrupciones del servicio.
   - **Mitigación:** Aplicar parches de seguridad y configurar limitaciones de acceso.
5. **CVE-2023-51385 (Criticidad: 6.5 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite la exfiltración de datos.
   - **Impacto:** Moderado, permite a un atacante obtener información sensible.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones para limitar la exposición de datos.
6. **CVE-2023-45802 (Criticidad: 5.9 - Media)**
   - **Descripción:** Vulnerabilidad en Apache HTTP Server que permite manipulación no autorizada de datos.
   - **Impacto:** Moderado, puede permitir alteración no autorizada de datos.
   - **Mitigación:** Actualizar Apache HTTP Server y aplicar configuraciones de seguridad adecuadas.
7. **CVE-2022-23307 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en Apache Log4j 2.x que permite ejecución remota de código.
   - **Impacto:** Alto, permite a un atacante ejecutar comandos arbitrarios en el servidor afectado.
   - **Mitigación:** Actualizar Apache Log4j a la versión más reciente que corrige esta vulnerabilidad.
8. **CVE-2019-0190 (Criticidad: 7.5 - Alta)**
   - **Descripción**: Vulnerabilidad en Apache HTTP Server que permite ataques de denegación de servicio.
   - **Impacto:** Moderado, puede causar interrupciones del servicio.
   - **Mitigación:** Aplicar parches de seguridad y configurar limitaciones de acceso adecuadas.
9. **CVE-2020-26116 (Criticidad: 6.8 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite a un atacante remoto realizar ataques de fuerza bruta.
   - **Impacto:** Moderado, permite intentos de acceso no autorizado.

- **Mitigación:** Configurar restricciones de acceso y aplicar políticas de autenticación robustas.

10. CVE-2018-11776 (Criticidad: 9.8 - Crítica)

- **Descripción:** Vulnerabilidad en Apache Struts que permite ejecución remota de código.
- **Impacto:** Alto, podría permitir a un atacante comprometer el servidor si no se mitigan los riesgos.
- **Mitigación:** Actualizar Apache Struts a la última versión y aplicar configuraciones de seguridad adicionales.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.23

Puertos Abiertos y Servicios Asociados

1. **13/tcp - daytime**: Servicio que devuelve la fecha y hora actuales. Este servicio es poco común en sistemas modernos y puede deshabilitarse si no es necesario.
2. **22/tcp - ssh - OpenSSH 8.1, protocolo 2.0**: Servicio SSH utilizado para conexiones seguras. Es fundamental mantener este servicio actualizado para evitar posibles vulnerabilidades.
3. **25/tcp - smtp - ESMTP Sendmail**: Servidor de correo que puede ser vulnerable si no se configura adecuadamente. Asegúrate de aplicar las mejores prácticas de seguridad y mantener actualizado el software.
4. **37/tcp - time:** Protocolo que devuelve la hora en segundos desde 1900. Raramente utilizado en sistemas modernos y podría ser cerrado si no es necesario.
5. **111/tcp - rpcbind:** Servicio utilizado por varios servicios RPC para identificar puertos. Debe estar correctamente configurado y limitado a sistemas autorizados para evitar explotación.
6. **199/tcp - smux:** Protocolo de multiplexer de SNMP. Asegúrate de que esté configurado de manera segura y que el acceso esté restringido.
7. **657/tcp - rmc:** Protocolo de Control Remoto. Debe estar configurado adecuadamente para evitar accesos no autorizados.
8. **1334/tcp - writesrv:** Servicio de escritura que tiene un uso limitado en redes modernas. Podría deshabilitarse si no es necesario.
9. **2049/tcp - nfs:** Sistema de archivos de red utilizado para compartir archivos a través de la red. Necesita estar configurado con las opciones de seguridad adecuadas para evitar accesos no autorizados.
10. **2223/tcp - rockwell-csp2**: Servicio específico para sistemas Rockwell. Debe ser restringido a sistemas autorizados para evitar acceso no deseado.
11. **2224/tcp - efi-mg:** Servicio EFI utilizado para la gestión de interfaces. Asegúrate de que esté protegido adecuadamente.
12. **6112/tcp - tcpwrapped**: Indica que el puerto está protegido por TCP Wrapper, una medida adicional de seguridad. Se debe asegurar que las reglas de acceso sean adecuadas.
13. **6181/tcp - unknown:** Puerto abierto desconocido, es importante investigar y asegurar este puerto para evitar posibles riesgos.
14. **10050/tcp - tcpwrapped:** Protocolo de envoltura de TCP, que proporciona una capa adicional de seguridad. Se debe revisar la configuración de TCP Wrapper para asegurar que esté correctamente implementada.

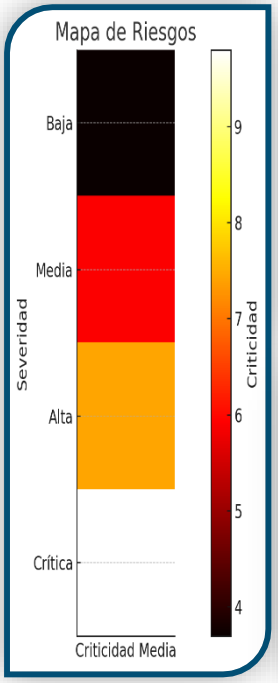
15. **16191/tcp - unknown:** Puerto abierto desconocido, se recomienda investigar y asegurar este puerto para evitar vulnerabilidades.
16. **32768/tcp - filenet-tms:** Servicio de gestión de transacciones FileNet, que debe estar protegido adecuadamente para evitar compromisos.
17. **32769/tcp - nlockmgr:** Gestor de bloqueo de NFS, que debe estar configurado para la seguridad y limitado a hosts autorizados.
18. **32770/tcp - nsm_addrand:** Servicio de administración de direcciones NSM, se debe configurar correctamente para evitar accesos no autorizados.
19. **32775/tcp - mountd:** Servicio de montaje NFS, debe estar configurado para minimizar los riesgos y limitado a sistemas autorizados.
20. **33682/tcp - unknown:** Puerto abierto desconocido, es importante investigar y asegurar este puerto para evitar posibles riesgos.

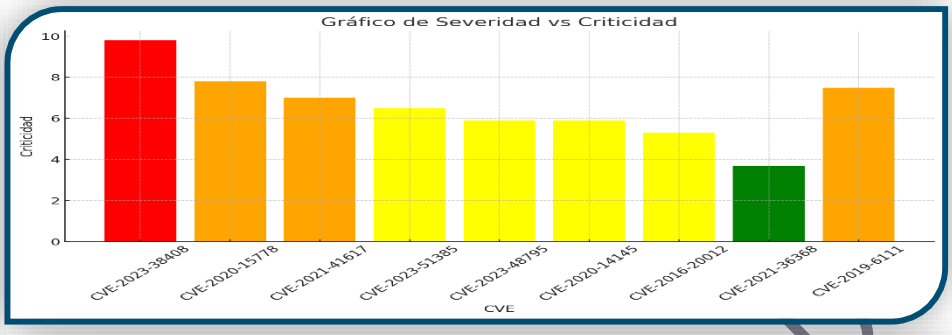
Vulnerabilidades Detectadas (CVEs)

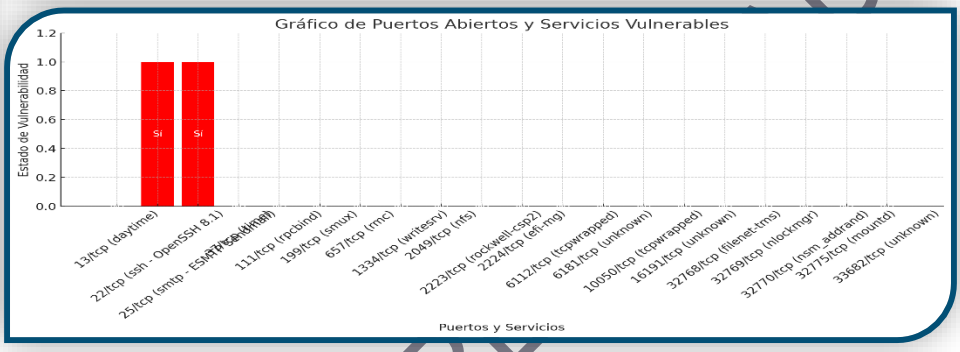
1. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.1 que permite la ejecución remota de código.
   - **Impacto:** Alto, permite a un atacante comprometer el servidor SSH.
   - **Mitigación**: Actualizar OpenSSH a la última versión disponible y restringir el acceso SSH solo a IPs de confianza.
2. **CVE-2020-15778 (Criticidad: 7.8 - Alta)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.1 que permite la ejecución remota de comandos a través de caracteres de escape.
   - **Impacto:** Alto, permite a un atacante remoto ejecutar comandos arbitrarios.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones para restringir el uso de caracteres peligrosos.
3. **CVE-2021-41617 (Criticidad: 7.0 - Alta)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite eludir restricciones de seguridad.
   - **Impacto:** Moderado, puede permitir acceso no autorizado.
   - **Mitigación:** Aplicar parches de seguridad y revisar configuraciones de acceso.
4. **CVE-2023-51385 (Criticidad: 6.5 - Media)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite la exfiltración de datos.
   - **Impacto:** Moderado, permite a un atacante obtener información sensible.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones para limitar la exposición de datos.

5. **CVE-2023-48795 (Criticidad: 5.9 - Media)**
    - **Descripción**: Vulnerabilidad en OpenSSH que permite manipulación no autorizada de datos.
    - **Impacto**: Moderado, puede permitir alteración no autorizada de datos.
    - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones de seguridad adecuadas.
6. **CVE-2020-14145 (Criticidad: 5.9 - Media)**
    - **Descripción:** Vulnerabilidad en OpenSSH que permite manipulación no autorizada de datos.
    - **Impacto**: Moderado, puede permitir alteración no autorizada de datos.
    - **Mitigación**: Actualizar OpenSSH y aplicar configuraciones de seguridad adecuadas.
7. **CVE-2016-20012 (Criticidad: 5.3 - Media)**
    - **Descripción:** Vulnerabilidad en OpenSSH que permite manipulación no autorizada de configuraciones.
    - **Impacto:** Moderado, puede permitir a un atacante modificar configuraciones.
    - **Mitigación:** Aplicar parches de seguridad y revisar configuraciones de acceso.
8. **CVE-2021-36368 (Criticidad: 3.7 - Baja)**
    - **Descripción:** Vulnerabilidad en OpenSSH que permite técnicas de bypass de seguridad.
    - **Impacto:** Bajo, permite a un atacante eludir algunas restricciones de seguridad.
    - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones para mejorar la seguridad.
9. **CVE-2019-6111 (Criticidad: 7.5 - Alta)**
    - **Descripción**: Vulnerabilidad en OpenSSH SCP que permite la manipulación de archivos. Un atacante podría engañar al usuario para que descargue archivos maliciosos.
    - **Impacto**: Alto, puede permitir la manipulación no autorizada de archivos.
    - **Mitigación**: Actualizar OpenSSH a la versión más reciente y deshabilitar SCP si no es necesario.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.30

Puertos Abiertos y Servicios Asociados

1. **13/tcp - daytime:** Servicio que devuelve la fecha y hora actuales. Puede ser deshabilitado si no es necesario en entornos modernos.
2. **22/tcp - ssh:** Servicio de SSH, utilizando OpenSSH 8.1 con protocolo 2.0. Se recomienda mantener actualizado y restringir el acceso solo a IPs de confianza**.**
3. **25/tcp - smtp:** Servicio de correo ESMTP Sendmail, que puede ser vulnerable si no se configura adecuadamente. Se requiere aplicar las mejores prácticas de seguridad**.**
4. **37/tcp - time:** Servicio que devuelve la hora en segundos desde 1900, poco utilizado en sistemas actuales.
5. **111/tcp - rpcbind:** Servicio utilizado por RPC para identificar puertos. Debe estar adecuadamente configurado y protegido.
6. **199/tcp - smux:** Protocolo multiplexer de SNMP. Se recomienda restringir su acceso.
7. 514/tcp - tcpwrapped: Protocolo de envoltura de TCP, que proporciona una capa adicional de seguridad.
8. **657/tcp - rmc:** Servicio de gestión remota, debe ser configurado adecuadamente.
9. **1334/tcp - writesrv:** Servicio de escritura, poco común en sistemas modernos, podría deshabilitarse si no es necesario.
10. **6112/tcp - tcpwrapped:** Otro puerto protegido por TCP Wrapper.
11. **6181/tcp, 8226/tcp, 9228/tcp, 16191/tcp - unknown:** Puertos abiertos desconocidos que requieren investigación y aseguramiento.
12. **32768/tcp - filenet-tms:** Sistema de gestión de transacciones de FileNet.
13. **32769/tcp - nlockmgr:** Gestor de bloqueo de NFS, requiere configurarse adecuadamente.
14. **32770/tcp - nsm_addrand:** Servicio de administración de direcciones de NSM.
15. **32771/tcp - ttdbserverd:** Servicio RPC utilizado por ttdbserverd.

Vulnerabilidades Detectadas (CVEs)

1. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción**: Vulnerabilidad en OpenSSH 8.1 que permite la ejecución remota de código.
   - **Impacto**: Alto, permite comprometer el servidor SSH**.**
   - **Mitigación:** Actualizar OpenSSH y restringir acceso SSH solo a IPs confiables.
2. **CVE-2020-15778 (Criticidad: 7.8 - Alta)**
   - **Descripción:** Permite la ejecución remota de comandos a través de caracteres de escape.
   - **Impacto:** Alto, permite ejecutar comandos arbitrarios.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones de seguridad adicionales**.**

3. **CVE-2021-41617 (Criticidad: 7.0 - Alta)**
    - **Descripción**: Permite eludir restricciones de seguridad en OpenSSH.
    - **Impacto**: Moderado, puede permitir accesos no autorizados.
    - **Mitigación:** Aplicar parches y revisar configuraciones de seguridad.
4. **CVE-2023-51385 (Criticidad: 6.5 - Media)**
    - **Descripción:** Permite la exfiltración de datos**.**
    - **Impacto:** Moderado, puede permitir que un atacante obtenga información sensible**.**
    - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones de seguridad.
5. **CVE-2023-48795 (Criticidad: 5.9 - Media)**
    - **Descripción:** Manipulación no autorizada de datos en OpenSSH.
    - **Impacto:** Moderado, permite alteración de datos.
    - **Mitigación:** Aplicar parches de seguridad**.**
6. **CVE-2020-14145 (Criticidad: 5.9 - Media)**
    - **Descripción:** Manipulación no autorizada de datos**.**
    - **Impacto:** Moderado, puede permitir alteración no autorizada de datos**.**
    - **Mitigación:** Actualizar OpenSSH y configurar adecuadamente.
7. **CVE-2016-20012 (Criticidad: 5.3 - Media)**
    - **Descripción**: Manipulación de configuraciones en OpenSSH**.**
    - **Impacto:** Moderado, puede permitir cambios no autorizados**.**
    - **Mitigación:** Aplicar parches y revisar configuraciones**.**
8. **CVE-2021-36368 (Criticidad: 3.7 - Baja)**
    - **Descripción:** Bypass de seguridad en OpenSSH**.**
    - **Impacto:** Bajo, permite eludir restricciones.
    - **Mitigación:** Actualizar OpenSSH y mejorar configuraciones**.**
9. **CVE-2019-6111 (Criticidad: 7.5 - Alta)**
    - **Descripción:** Vulnerabilidad en OpenSSH SCP que permite la manipulación de archivos. Un atacante puede engañar al usuario para descargar archivos maliciosos.
    - **Impacto:** Alto, permite manipulación no autorizada de archivos**.**
    - **Mitigación:** Actualizar OpenSSH y revisar configuraciones de SCP. Deshabilitar SCP si no es necesario.

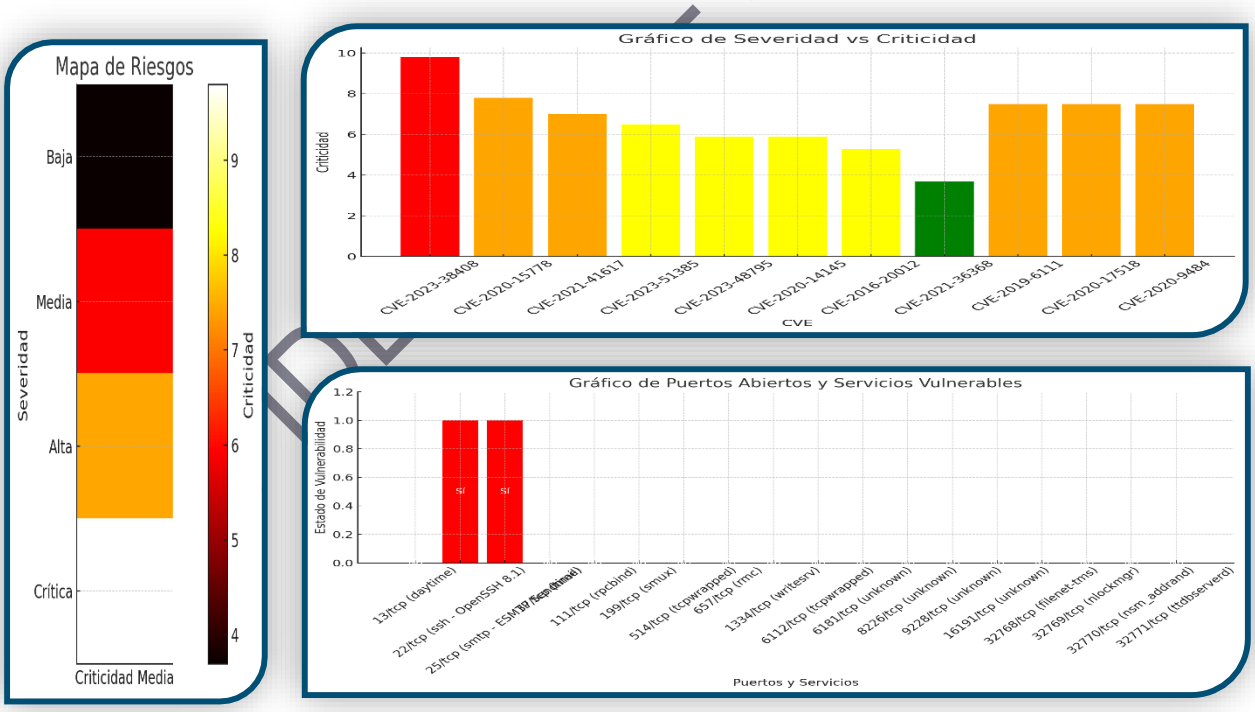
10. CVE-2020-17518 (Criticidad: 7.5 - Alta)

- **Descripción:** Vulnerabilidad en Apache HTTP Server que puede permitir la ejecución remota de código a través de un ataque de denegación de servicio.
- **Impacto:** Alto, permite que un atacante interrumpa el servicio o ejecute código malicioso.
- **Mitigación:** Aplicar parches de seguridad para Apache HTTP Server y revisar configuraciones de seguridad adicionales.

11. CVE-2020-9484 (Criticidad: 7.5 - Alta)

- **Descripción:** Vulnerabilidad en Apache Tomcat que podría permitir la ejecución remota de código mediante manipulación de sesiones.
- **Impacto:** Alto, permite comprometer aplicaciones que utilicen Tomcat.
- **Mitigación:** Actualizar Apache Tomcat y revisar las políticas de seguridad relacionadas con las sesiones.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.33

Puertos Abiertos y Servicios Asociados

1. **42/tcp - tcpwrapped:** Servicio envuelto por TCP Wrapper, lo que significa que el acceso a este puerto está restringido por una capa adicional de seguridad.
2. **53/tcp - domain:** Servidor DNS Simple DNS Plus. Este servicio es crucial para la resolución de nombres de dominio, pero puede ser vulnerable si no se configura adecuadamente.
3. **80/tcp - http:** Servicio HTTP con Microsoft IIS 8.5. Es importante mantener actualizado IIS para evitar vulnerabilidades conocidas.
4. **88/tcp - kerberos-sec:** Servicio de Kerberos en Microsoft Windows, utilizado para la autenticación segura en redes.
5. **135/tcp - msrpc:** Protocolo RPC de Microsoft Windows, utilizado para comunicación entre procesos. Este puerto es crítico y debe estar bien protegido.
6. **139/tcp - netbios-ssn:** Servicio NetBIOS para compartir archivos e impresoras en redes locales. Es vulnerable si se deja abierto a redes no seguras.
7. **389/tcp - ldap:** Servicio LDAP para Active Directory. Este servicio es vital para la gestión de usuarios, pero debe estar adecuadamente asegurado.
8. **443/tcp - http:** Servicio HTTPS de VMware Server configurado con Microsoft IIS. Se recomienda aplicar buenas prácticas de seguridad para la configuración HTTPS.
9. **445/tcp - microsoft-ds:** Servicio para compartir archivos de Microsoft (SMB). Este puerto es conocido por ser un vector de ataque para vulnerabilidades críticas como WannaCry o EternalBlue.
10. **464/tcp - kpasswd5:** Servicio de Kerberos utilizado para cambiar contraseñas en Active Directory.
11. **593/tcp - ncacn_http:** RPC sobre HTTP, debe ser configurado correctamente para minimizar riesgos.
12. **636/tcp - tcpwrapped:** Otro puerto envuelto por TCP Wrapper, lo que agrega seguridad al servicio.
13. **903/tcp, 913/tcp - vmware-auth:** Daemon de autenticación de VMware. Utilizado para autenticar conexiones de administración.
14. **3268/tcp - ldap:** Otro servicio LDAP para Active Directory, utilizado para consultas globales.
15. **3389/tcp - ms-wbt-server:** Protocolo de escritorio remoto (RDP) de Microsoft. Este puerto debe ser configurado con precauciones adicionales, como el uso de autenticación fuerte y restricciones IP.
16. **5985/tcp - http:** Servicio HTTP de Microsoft HTTPAPI 2.0 utilizado para SSDP y UPnP.
17. **8000/tcp - http-alt:** Puerto alternativo HTTP abierto, se recomienda verificar qué servicio está utilizando este puerto.
18. **8530/tcp, 8531/tcp - http:** Servicio Microsoft IIS 8.5. Se recomienda mantener este servicio actualizado.

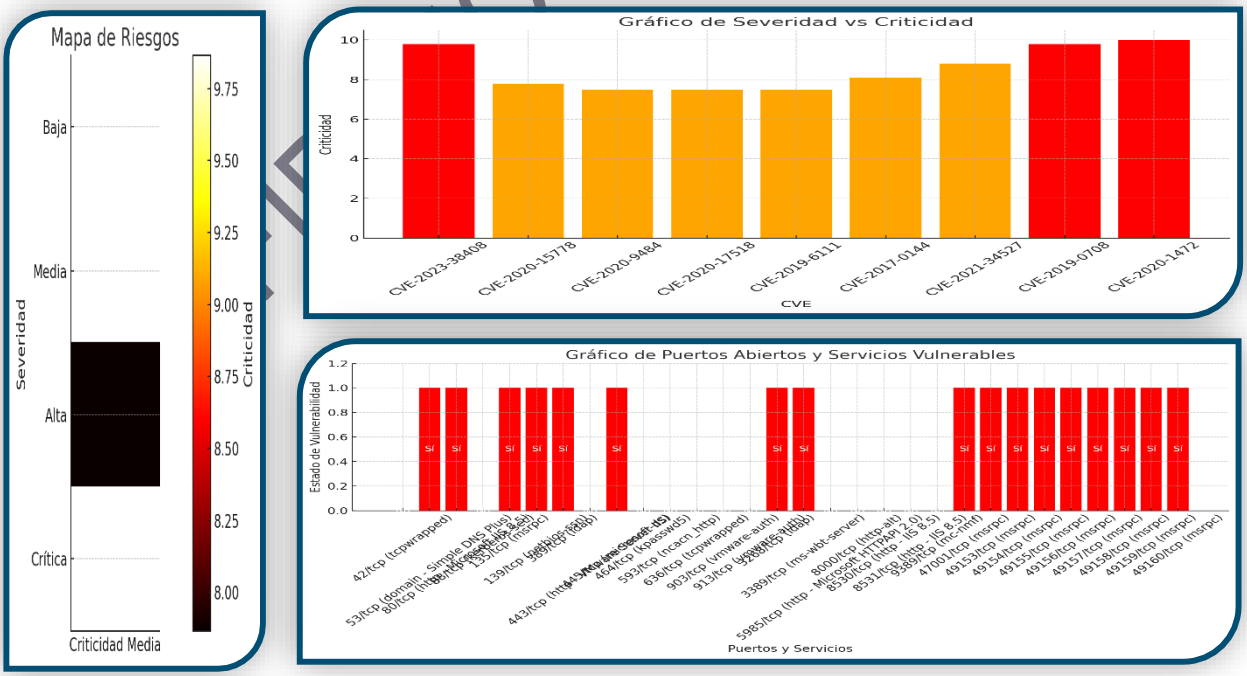
19. **9389/tcp - mc-nmf:** .NET Message Framing, utilizado por servicios de Microsoft .NET.
20. **47001/tcp, 49153/tcp a 60532/tcp - msrpc:** Varios puertos RPC de Microsoft. Estos puertos son comunes en redes Windows y deben estar debidamente configurados para evitar posibles exploits.

Vulnerabilidades Detectadas (CVEs)

1. **CVE-2023-38408 (Criticidad: 9.8 - Crítica)**
   - **Descripción:** Vulnerabilidad en OpenSSH 8.1 que permite la ejecución remota de código.
   - **Impacto:** Alto, permite comprometer el servidor SSH.
   - **Mitigación**: Actualizar OpenSSH y restringir acceso SSH solo a IPs confiables.
2. **CVE-2020-15778 (Criticidad: 7.8 - Alta)**
   - **Descripción:** Vulnerabilidad en OpenSSH que permite la ejecución remota de comandos.
   - **Impacto:** Alto, permite ejecutar comandos arbitrarios en el sistema.
   - **Mitigación:** Actualizar OpenSSH y aplicar configuraciones de seguridad adicionales.
3. **CVE-2020-9484 (Criticidad: 7.5 - Alta)**
   - **Descripción**: Vulnerabilidad en Apache Tomcat que permite la ejecución remota de código mediante manipulación de sesiones.
   - **Impacto:** Alto, compromete aplicaciones web que utilicen Tomcat.
   - **Mitigación**: Actualizar Apache Tomcat y revisar las políticas de seguridad relacionadas con sesiones.
4. **CVE-2020-17518 (Criticidad: 7.5 - Alta)**
   - **Descripción:** Vulnerabilidad en Apache HTTP Server que permite ataques de denegación de servicio y ejecución remota de código.
   - **Impacto:** Alto, interrumpe el servicio o permite la ejecución de código malicioso.
   - **Mitigación:** Aplicar parches de seguridad y revisar las configuraciones.
5. **CVE-2019-6111 (Criticidad: 7.5 - Alta)**
   - **Descripción**: Vulnerabilidad en SCP de OpenSSH que permite la manipulación de archivos. Un atacante podría engañar a un usuario para descargar archivos maliciosos.
   - **Impacto:** Alto, manipulación no autorizada de archivos.
   - **Mitigación:** Actualizar OpenSSH y revisar la configuración de SCP.
6. **CVE-2017-0144 (WannaCry) (Criticidad: 8.1 - Alta)**
   - **Descripción**: Vulnerabilidad en SMBv1 explotada por ransomware como WannaCry.
   - **Impacto**: Alta, permite la ejecución remota de código.
   - **Mitigación**: Deshabilitar SMBv1 y aplicar parches de seguridad.

7. **CVE-2021-34527 (PrintNightmare) (Criticidad: 8.8 - Alta)**
    - **Descripción**: Vulnerabilidad en el servicio de impresión de Windows que permite la ejecución remota de código.
    - **Impacto:** Alto, permite comprometer remotamente el sistema.
    - **Mitigación:** Aplicar parches y restringir acceso al servicio de impresión.
8. **CVE-2019-0708 (BlueKeep) (Criticidad: 9.8 - Crítica)**
    - **Descripción**: Vulnerabilidad crítica en RDP que permite la ejecución remota de código sin autenticación.
    - **Impacto**: Alto, puede permitir la toma de control del sistema.
    - **Mitigación:** Aplicar parches y asegurar el acceso a RDP con MFA.
9. **CVE-2020-1472 (ZeroLogon) (Criticidad: 10.0 - Crítica)**
    - **Descripción:** Vulnerabilidad en Netlogon que permite el control total de un controlador de dominio sin necesidad de credenciales.
    - **Impacto**: Crítico, permite la toma de control del dominio.
    - **Mitigación:** Aplicar parches y reforzar las políticas de acceso a controladores de dominio.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.42

Puertos Abiertos y Servicios Asociados

1. **21/tcp** - **ftp (Microsoft IIS ftpd)**: Servicio FTP expuesto, utilizado por Microsoft IIS. Es vulnerable si las credenciales no están cifradas. Se recomienda migrar a SFTP o FTPS.
2. **23/tcp** - **telnet**: Protocolo Telnet expuesto. Dado que Telnet transmite credenciales en texto claro, se recomienda reemplazarlo por SSH o deshabilitarlo si no es necesario.
3. **24/tcp** - **tcpwrapped**: Puerto protegido por TCP Wrapper, lo que añade una capa adicional de seguridad.
4. **80/tcp** - **http (Microsoft IIS 7.0)**: Servicio HTTP proporcionado por Microsoft IIS versión 7.0. Esta versión es vulnerable a múltiples ataques de ejecución remota de código, por lo que se recomienda actualizar a una versión más reciente.
5. **135/tcp** - **msrpc**: Protocolo RPC de Microsoft utilizado para la comunicación entre procesos en redes Windows. Este puerto es crítico y debe estar protegido con un firewall.
6. **139/tcp** - **netbios-ssn**: Servicio NetBIOS utilizado para compartir archivos en redes locales. Es un objetivo común para ataques y debe estar bloqueado si no es necesario.
7. **443/tcp** - **https (Microsoft IIS 7.0)**: Servicio HTTPS expuesto, que necesita verificación de las configuraciones de TLS/SSL para garantizar el uso de protocolos seguros y certificados actualizados.
8. **445/tcp** - **microsoft-ds**: Servicio SMB de Microsoft, susceptible a ataques como **EternalBlue** y **WannaCry** si no está parcheado.
9. **1723/tcp** - **pptp**: Protocolo de Túnel Punto a Punto (PPTP) utilizado para VPNs. PPTP es considerado inseguro y debería ser reemplazado por alternativas más seguras como L2TP o OpenVPN.
10. **3389/tcp** - **ms-wbt-server (RDP)**: Protocolo de Escritorio Remoto (RDP) de Microsoft. Se recomienda configurar autenticación fuerte, aplicar los parches de seguridad como **BlueKeep**, y restringir el acceso a direcciones IP confiables.
11. **5357/tcp** - **upnp**: Universal Plug and Play (UPnP). Este servicio es conocido por sus vulnerabilidades si no está bien configurado. Se recomienda deshabilitarlo si no es necesario.
12. **49152/tcp** a **53460/tcp** - **msrpc**: Múltiples puertos abiertos para el servicio de RPC de Microsoft. Estos puertos deben estar protegidos con firewall y accesos restringidos.

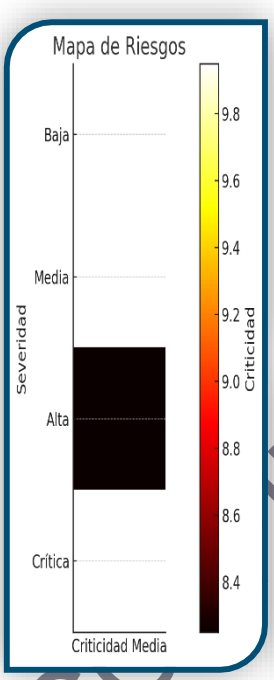
Vulnerabilidades Detectadas (CVEs)

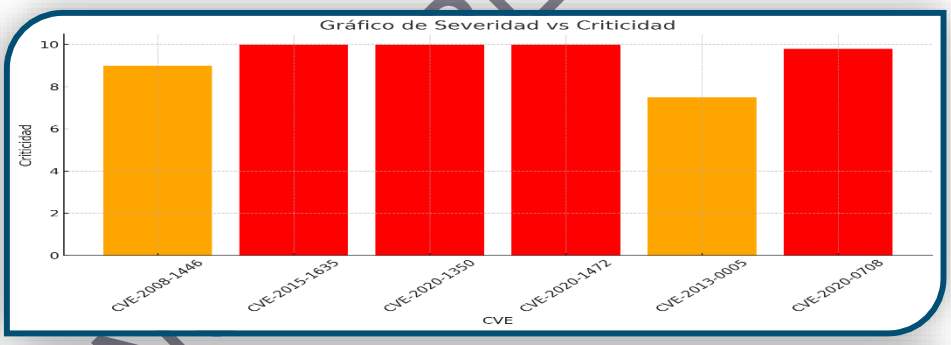
1. **CVE-2008-1446** (Criticidad: 9.0 - Alta)
    - **Descripción**: Vulnerabilidad en IIS 7.0 que permite la ejecución remota de código.
    - **Impacto**: Crítico, un atacante podría tomar el control del servidor.
    - **Mitigación**: Actualizar IIS a una versión más reciente y aplicar los parches correspondientes.
2. **CVE-2015-1635** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad en Microsoft IIS 7.0 que permite la ejecución remota de código a través de paquetes HTTP malformados.
    - **Impacto**: Crítico, permite la ejecución remota de código.
    - **Mitigación**: Aplicar parches y asegurarse de que el servicio HTTP esté configurado de manera segura.
3. **CVE-2020-1350 (SigRed)** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad en el servicio DNS de Windows Server que permite la ejecución remota de código.
    - **Impacto**: Crítico, un atacante puede comprometer el servidor DNS.
    - **Mitigación**: Aplicar los parches correspondientes y restringir el acceso al servicio DNS.
4. **CVE-2020-1472 (ZeroLogon)** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad en el protocolo Netlogon que permite la toma de control de un controlador de dominio sin autenticación.
    - **Impacto**: Crítico, un atacante puede tomar el control total de un dominio en redes Windows.
    - **Mitigación**: Aplicar los parches de seguridad de Microsoft y reforzar la seguridad en controladores de dominio.
5. **CVE-2013-0005** (Criticidad: 7.5 - Alta)
    - **Descripción**: Vulnerabilidad en IIS y .NET Framework que permite ataques de denegación de servicio (DoS).
    - **Impacto**: Moderado, un atacante puede interrumpir el servicio.
    - **Mitigación**: Aplicar parches y configurar las políticas de acceso adecuadas.
6. **CVE-2020-0708 (BlueKeep)** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad crítica en RDP que permite la ejecución remota de código sin autenticación.
    - **Impacto**: Crítico, un atacante puede tomar el control completo del servidor.
    - **Mitigación**: Aplicar los parches para BlueKeep y restringir el acceso a RDP mediante autenticación fuerte y MFA.

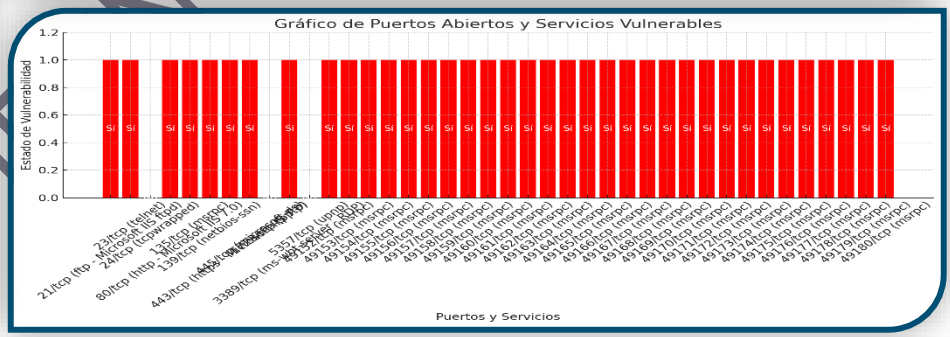
Recomendaciones Adicionales

- **Migrar a SFTP/FTPS**: El uso de FTP debe ser descontinuado y reemplazado por alternativas seguras como SFTP o FTPS.
- **Deshabilitar Telnet**: Reemplazar Telnet por SSH para garantizar la seguridad de las credenciales transmitidas.
- **Fortalecer el acceso RDP**: Implementar autenticación multifactor (MFA) para RDP y restringir el acceso a IPs confiables. Aplicar el parche **BlueKeep** (CVE-2020-0708).
- **Actualizar IIS**: Actualizar IIS 7.0 a una versión más reciente y asegurar las configuraciones TLS/SSL para minimizar las vulnerabilidades.
- **Deshabilitar SMBv1**: Deshabilitar SMBv1 para proteger el servidor contra ataques como **EternalBlue**.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.44

Puertos Abiertos y Servicios Asociados

1. **111/tcp** - **rpcbind**: Servicio RPC que ayuda a asignar puertos a otros servicios RPC. Es crítico proteger este servicio y limitar el acceso a redes internas seguras.
2. **135/tcp** - **msrpc**: Protocolo RPC de Microsoft, utilizado para la comunicación entre procesos en redes Windows. Este puerto es vulnerable a exploits si no está protegido adecuadamente.
3. **139/tcp** - **netbios-ssn**: Servicio NetBIOS utilizado para compartir archivos en redes locales. Debe ser configurado para evitar que sea expuesto a redes no confiables, ya que es vulnerable a ataques.
4. **445/tcp** - **microsoft-ds (SMB)**: Servicio SMB de Microsoft, conocido por vulnerabilidades críticas como **EternalBlue**. Es importante deshabilitar **SMBv1** y aplicar parches de seguridad para mitigar estos riesgos.
5. **3389/tcp** - **ms-wbt-server (RDP)**: Protocolo de Escritorio Remoto (RDP) de Microsoft, altamente susceptible a ataques si no está adecuadamente protegido. Se recomienda implementar **MFA** y restringir el acceso a direcciones IP confiables.
6. **5985/tcp** - **http (Microsoft HTTPAPI httpd)**: Servicio HTTP expuesto que utiliza WinRM para la administración remota. Se debe asegurar que las conexiones estén cifradas y limitar el acceso a redes seguras.
7. **607/tcp**, **635/tcp**, **787/tcp** - Servicios RPC adicionales. Estos puertos también deben ser restringidos para evitar la exposición a redes no confiables.
8. **5666/tcp**, **12489/tcp**, **10050/tcp** - **tcpwrapped**: Servicios protegidos con TCP Wrapper, lo cual añade una capa de seguridad, pero es importante asegurar que las configuraciones estén correctamente implementadas.
9. **Otros Puertos Abiertos**: Múltiples puertos adicionales relacionados con servicios RPC y HTTP. Se debe revisar la necesidad de estos puertos y cerrar aquellos que no sean necesarios para reducir la superficie de ataque.

Vulnerabilidades Detectadas (CVEs)

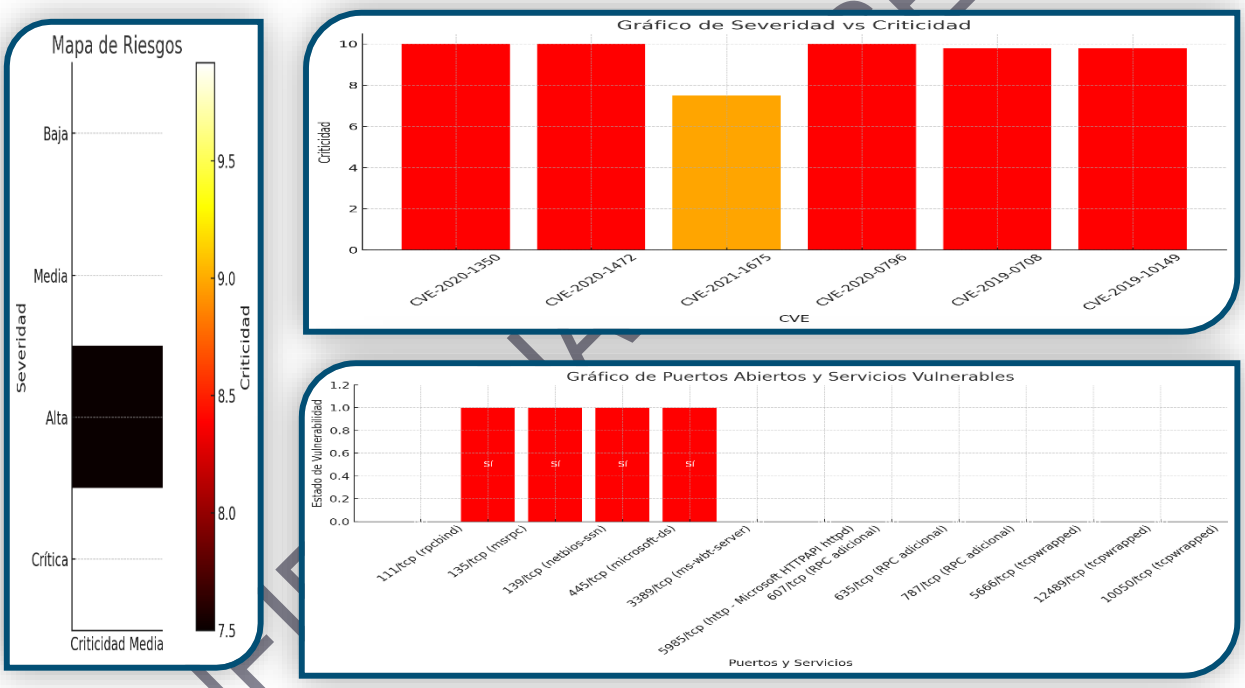
1. **CVE-2020-1350 (SigRed)** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad crítica en el servicio DNS de Windows Server que permite la ejecución remota de código.
    - **Impacto**: Crítico, un atacante podría tomar el control del servidor DNS.
    - **Mitigación**: Aplicar los parches de seguridad correspondientes y revisar las configuraciones de DNS.

2. **CVE-2020-1472 (ZeroLogon)** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad crítica en el protocolo Netlogon que permite la toma de control total de un controlador de dominio sin autenticación.
    - **Impacto**: Crítico, permite a un atacante tomar el control de un dominio.
    - **Mitigación**: Aplicar parches de seguridad de Microsoft y reforzar la seguridad de los controladores de dominio.
3. **CVE-2021-1675 (PrintNightmare)** (Criticidad: 7.5 - Alta)
    - **Descripción**: Vulnerabilidad en el servicio de impresión de Windows (Spooler) que permite la ejecución remota de código.
    - **Impacto**: Alto, permite a un atacante tomar control de un sistema vulnerable.
    - **Mitigación**: Aplicar el parche de seguridad y deshabilitar el servicio de impresión si no es necesario.
4. **CVE-2020-0796 (SMBGhost)** (Criticidad: 10.0 - Crítica)
    - **Descripción**: Vulnerabilidad crítica en SMBv3 que permite la ejecución remota de código.
    - **Impacto**: Crítico, permite la toma de control del sistema a través de SMBv3.
    - **Mitigación**: Aplicar los parches de seguridad correspondientes y asegurarse de que SMBv3 esté configurado correctamente.
5. **CVE-2019-0708 (BlueKeep)** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad crítica en RDP que permite la ejecución remota de código sin autenticación.
    - **Impacto**: Crítico, permite la toma de control completo del servidor a través de RDP.
    - **Mitigación**: Aplicar los parches de seguridad y reforzar el acceso a RDP con autenticación multifactor (MFA) y VPN.
6. **CVE-2019-10149 (Exim Mail Server)** (Criticidad: 9.8 - Crítica)
    - **Descripción**: Vulnerabilidad en Exim Mail Server que permite la ejecución remota de código.
    - **Impacto**: Alto, un atacante remoto puede ejecutar comandos arbitrarios en el servidor.
    - **Mitigación**: Actualizar Exim Mail Server a la versión más reciente que corrija esta vulnerabilidad.

Recomendaciones adicionales

- **Fortalecer SMB y RDP**: Implementar medidas de seguridad para SMB y RDP, deshabilitar SMBv1 y aplicar los parches de seguridad más recientes, incluyendo **BlueKeep** y **SMBGhost**.
- **Limitar el acceso a RPC y WinRM**: Asegurar que los servicios de administración remota, como RPC y WinRM, estén protegidos mediante TLS y solo accesibles desde redes internas seguras.
- **Parchear y revisar los servicios de impresión**: Deshabilitar el servicio de impresión si no es necesario y aplicar los parches correspondientes a **PrintNightmare**.
- **Actualizar Exim Mail Server**: Si se utiliza Exim Mail Server, es fundamental actualizarlo a la última versión disponible para evitar la explotación de vulnerabilidades críticas.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.84

Puertos Abiertos y Servicios Asociados

1. **22/tcp - ssh (OpenSSH 7.9p1 Debian 10+deb10u2, protocolo 2.0)**
    - **Descripción**: Servicio SSH utilizado para acceso remoto seguro. OpenSSH es crítico para la administración remota, pero es importante asegurarlo adecuadamente.
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución de comandos arbitrarios.
        - **CVE-2019-16905** (Criticidad: 7.8 - Alta): Escalada de privilegios locales.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
        - **CVE-2019-6110** (Criticidad: 6.8 - Media): Manipulación de archivos SCP.
2. **8009/tcp - ajp13 (Apache JServ Protocol, v1.3)**
    - **Descripción**: Puerto utilizado para la comunicación AJP entre servidores web Apache y servidores de aplicaciones.
    - **Vulnerabilidades**:
        - **CVE-2020-1938 (Ghostcat)** (Criticidad: 9.8 - Crítica): Vulnerabilidad que permite la lectura de archivos confidenciales.
        - **CVE-2018-11784** (Criticidad: 7.5 - Alta): Denegación de servicio.
3. **8181/tcp - http (WildFly Application Server, versiones 15.0.0 - 29.0.1)**
    - **Descripción**: Servicio HTTP para el servidor de aplicaciones WildFly. Es importante revisar las configuraciones de seguridad.
    - **Recomendación**: Revisar configuraciones de TLS/SSL y aplicar parches de seguridad.
4. **8443/tcp - http (WildFly Application Server, versiones 15.0.0 - 29.0.1)**
    - **Descripción**: Servicio HTTPS utilizado por WildFly para comunicaciones seguras.
    - **Recomendación**: Asegurar el uso de certificados SSL/TLS válidos y actualizados.
5. **9991/tcp - http (JBoss WildFly web console)**
    - **Descripción**: Consola web de administración de JBoss WildFly, que permite la gestión del servidor.
    - **Recomendación**: Restringir el acceso a esta consola solo a redes internas confiables y aplicar medidas de autenticación adicionales.

6. **10050/tcp - Zabbix Agent**
    - **Descripción**: Puerto utilizado por Zabbix para la monitorización del servidor.

- **Recomendación**: Limitar el acceso de este puerto solo a servidores de monitorización autorizados mediante firewall y reglas de acceso.

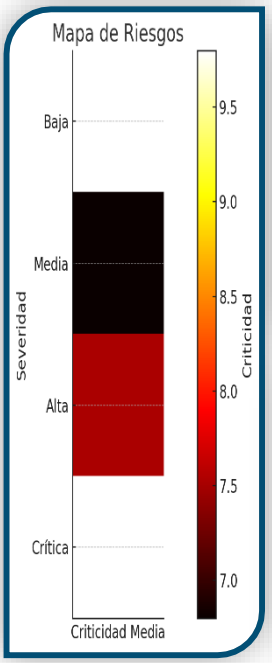
Vulnerabilidades Críticas Detectadas

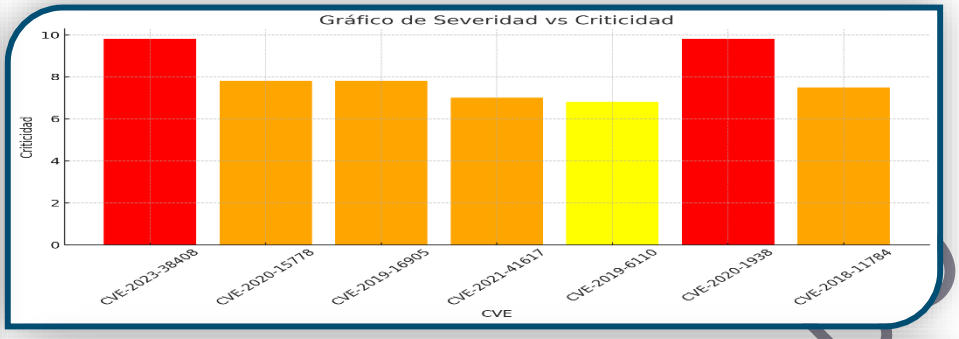
1. **CVE-2023-38408** (SSH Exploit) - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en OpenSSH que permite la ejecución remota de código.
   - **Mitigación**: Actualizar OpenSSH y aplicar medidas de protección como MFA.
2. **CVE-2020-15778** (SSH Exploit) - **Criticidad: 7.8 - Alta**
   - **Descripción**: Permite ejecutar comandos arbitrarios en sistemas remotos.
   - **Mitigación**: Aplicar parches y revisar las configuraciones de acceso SSH.
3. **CVE-2020-1938 (Ghostcat)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en el protocolo AJP que permite la lectura de archivos confidenciales en el servidor.
   - **Mitigación**: Deshabilitar o asegurar el puerto AJP y restringir el acceso a redes internas.
4. **CVE-2019-16905** (SSH Escalada de Privilegios) - **Criticidad: 7.8 - Alta**
   - **Descripción**: Escalada de privilegios locales en OpenSSH.
   - **Mitigación**: Aplicar las actualizaciones necesarias y restringir el acceso SSH.
5. **CVE-2021-41617** (Denegación de Servicio en SSH) - **Criticidad: 7.0 - Alta**
   - **Descripción**: Vulnerabilidad que permite realizar ataques de denegación de servicio a través de OpenSSH.
   - **Mitigación**: Actualizar OpenSSH y asegurar el acceso con políticas de seguridad más estrictas.

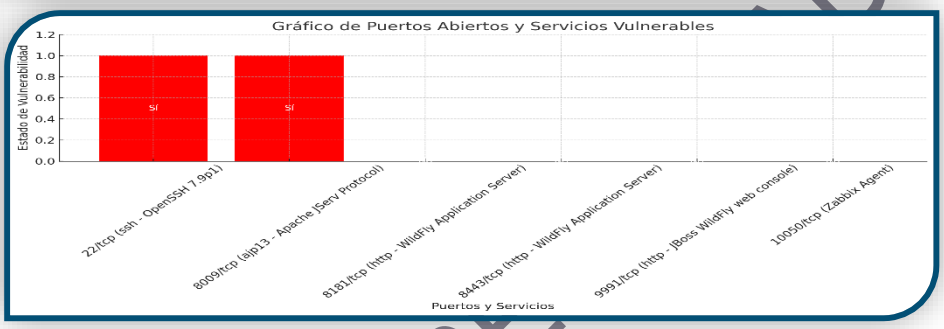
Recomendaciones de Seguridad

- **Actualizar OpenSSH**: Debido a las múltiples vulnerabilidades críticas detectadas, es fundamental actualizar OpenSSH a la última versión disponible y restringir el acceso SSH a IPs confiables.
- **Asegurar AJP**: El protocolo **AJP** (puerto 8009/tcp) debe ser deshabilitado si no es necesario o configurado adecuadamente para limitar el acceso solo a redes internas seguras.
- **Refuerzo de la Consola de Administración de WildFly**: La consola de administración en **9991/tcp** debe estar protegida mediante autenticación fuerte y accesible solo desde redes internas confiables.
- **Revisar la Configuración de WildFly y Tomcat**: Asegurarse de que los servidores de aplicaciones, como WildFly y Tomcat, estén configurados con medidas de seguridad adecuadas para evitar accesos no autorizados o fugas de datos.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.91

Puertos Abiertos y Servicios Asociados

1. **13/tcp** - **daytime**
    - **Descripción**: Protocolo que devuelve la fecha y hora actual.
    - **Recomendación**: Este puerto rara vez se utiliza y puede cerrarse si no es necesario.
2. **22/tcp** - **ssh (OpenSSH 8.1, protocolo 2.0)**
    - **Descripción**: Servicio SSH utilizado para el acceso remoto seguro.
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución de comandos arbitrarios.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
    - **Recomendación**: Actualizar a la última versión de OpenSSH, aplicar autenticación de múltiples factores (MFA) y usar claves SSH en lugar de contraseñas.
3. **25/tcp** - **nagios-nsca**
    - **Descripción**: Servicio utilizado para la transmisión de mensajes en el sistema de monitorización Nagios.
    - **Recomendación**: Asegurar el tráfico mediante TLS y autenticación segura.
4. **37/tcp** - **time**
    - **Descripción**: Protocolo de hora, similar a **daytime**, ya en desuso.
    - **Recomendación**: Desactivar este puerto si no es necesario.
5. **111/tcp** - **rpcbind**
    - **Descripción**: Servicio que asigna direcciones para los servicios RPC.
    - **Vulnerabilidades**: Si no está protegido, puede ser un vector de ataque.
    - **Recomendación**: Restringir el acceso al puerto solo a redes internas seguras.
6. **2049/tcp** - **nfs (Network File System)**
    - **Descripción**: Protocolo que permite compartir archivos entre servidores.
    - **Vulnerabilidades**: Si está mal configurado, NFS puede permitir acceso no autorizado a archivos compartidos.
    - **Recomendación**: Limitar el acceso mediante listas de control de acceso (ACL) y asegurarse de que solo hosts autorizados puedan conectarse.
7. **31000/tcp** hasta **31021/tcp** - **java-rmi (Remote Method Invocation)**
    - **Descripción**: Puerto utilizado para la invocación remota de métodos en aplicaciones Java.

- **Vulnerabilidades**: Existen riesgos de ataques de deserialización si no está configurado correctamente.
- **Recomendación**: Restringir el acceso solo a redes internas y aplicar configuraciones de seguridad en los servicios Java RMI.

Vulnerabilidades Críticas Detectadas

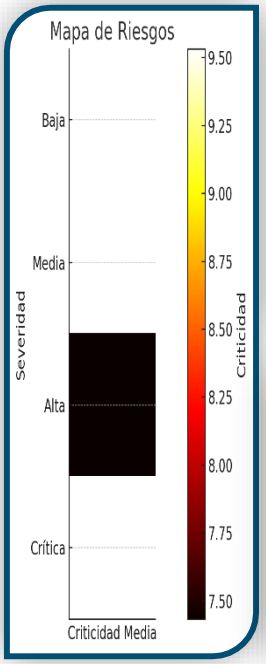
1. **CVE-2023-38408 (SSH Exploit)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en OpenSSH.
   - **Mitigación**: Actualizar OpenSSH y habilitar autenticación de múltiples factores (MFA).
2. **CVE-2020-15778 (SSH Exploit)** - **Criticidad: 7.8 - Alta**
   - **Descripción**: Permite la ejecución de comandos arbitrarios en sistemas remotos.
   - **Mitigación**: Actualizar OpenSSH a la última versión y revisar configuraciones de acceso SSH.
3. **CVE-2021-41617 (SSH)** - **Criticidad: 7.0 - Alta**
   - **Descripción**: Vulnerabilidad que permite ataques de denegación de servicio.
   - **Mitigación**: Aplicar parches de seguridad a OpenSSH.
4. **CVE-2020-1938 (Ghostcat)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en Apache Tomcat y su conector AJP que permite la lectura de archivos confidenciales en el servidor.
   - **Mitigación**: Deshabilitar o asegurar el puerto AJP y restringir el acceso a redes internas.
5. **CVE-2021-45046 (Log4Shell)** - **Criticidad: 9.0 - Crítica**
   - **Descripción**: Vulnerabilidad en Apache Log4j que permite la ejecución remota de código a través de la deserialización.
   - **Mitigación**: Actualizar a la versión más reciente de Log4j (2.17 o superior).
6. **CVE-2018-11784 (Apache JServ)** - **Criticidad: 7.5 - Alta**
   - **Descripción**: Vulnerabilidad en Apache JServ que puede causar una denegación de servicio.
   - **Mitigación**: Aplicar los parches de seguridad más recientes.

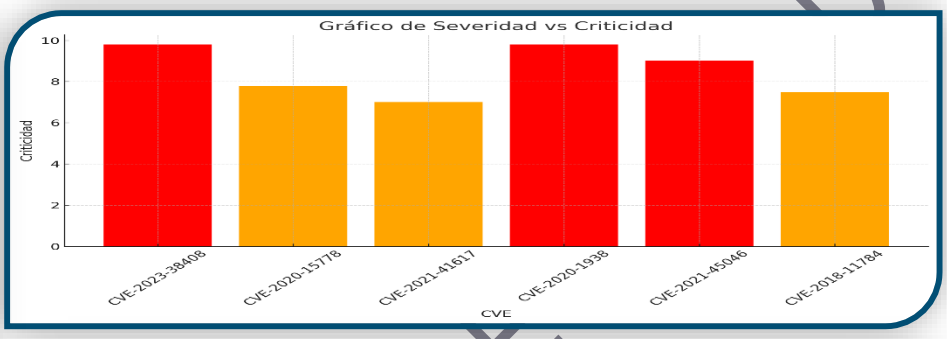
Recomendaciones de Seguridad

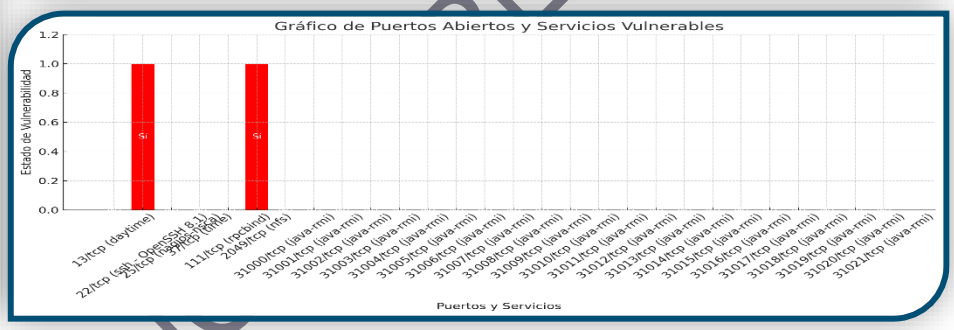
- **Cerrar o restringir puertos innecesarios**: Puertos como **13/tcp (daytime)** y **37/tcp (time)** deben cerrarse si no son esenciales.
- **Fortalecer NFS**: Configurar correctamente las exportaciones de NFS, limitando el acceso solo a hosts autorizados mediante listas de control de acceso (ACL) y asegurarse de que los archivos sensibles no estén expuestos.

- **Revisar la configuración de Java RMI**: Restringir el acceso a redes internas y aplicar políticas de seguridad adicionales para prevenir ataques de deserialización maliciosa.
- **Actualizar OpenSSH**: Actualizar OpenSSH y habilitar autenticación de múltiples factores (MFA).
- **Aplicar parches de seguridad para Apache Tomcat y Log4j**: Actualizar Apache Tomcat y Log4j a las versiones más recientes para mitigar vulnerabilidades como **Ghostcat** y **Log4Shell**.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.93

Puertos Abiertos y Servicios Asociados

1. **22/tcp - ssh (OpenSSH 8.1, protocolo 2.0)**
    - **Descripción**: Servicio SSH utilizado para acceso remoto seguro.
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución de comandos arbitrarios.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
    - **Recomendación**: Actualizar OpenSSH a la última versión, habilitar autenticación de múltiples factores (MFA) y usar claves SSH en lugar de contraseñas. Implementar medidas de seguridad como **Fail2Ban** para mitigar ataques de fuerza bruta.
2. **25/tcp - smtp (Sendmail)**
    - **Descripción**: Servicio de correo electrónico utilizado para el envío de correos a través de SMTP.
    - **Vulnerabilidades Detectadas**: Ninguna crítica específica.
    - **Recomendación**: Configurar Sendmail para evitar que se convierta en un relé abierto (open relay). Implementar autenticación TLS y políticas de seguridad como SPF y DKIM para proteger contra el uso indebido del servidor de correo.
3. **111/tcp - rpcbind**
    - **Descripción**: Servicio que asigna direcciones para los servicios RPC. Es un componente crítico en entornos distribuidos.
    - **Recomendación**: Restringir el acceso a rpcbind a redes internas confiables y utilizar reglas de firewall para limitar el acceso a este puerto.
4. **2049/tcp - nfs (Network File System)**
    - **Descripción**: Sistema de archivos distribuido que permite compartir archivos entre servidores.
    - **Vulnerabilidades**: Si no se configura adecuadamente, NFS puede exponer archivos a usuarios no autorizados.
    - **Recomendación**: Configurar listas de control de acceso (ACL) para limitar el acceso a hosts autorizados y aplicar medidas de autenticación basadas en Kerberos si es posible.
5. **1109/tcp - http (Jetty 6.1.x)**
    - **Descripción**: Servidor web Jetty, utilizado para servir aplicaciones web.
    - **Vulnerabilidades**:

- **CVE-2009-5049** (Criticidad: 6.1 - Media): Fuga de información.
- **CVE-2009-5048** (Criticidad: 6.1 - Media): Vulnerabilidad que permite ataques de denegación de servicio.

- **Recomendación**: Actualizar Jetty a una versión más reciente que mitigue estas vulnerabilidades y asegurar que las aplicaciones web estén protegidas contra ataques comunes como inyecciones y ataques de denegación de servicio.

6. **Java RMI (Remote Method Invocation)**
   - **Descripción**: Protocolo de invocación remota de métodos en Java. Detectado en múltiples puertos.
   - **Vulnerabilidades**: Las versiones más antiguas de Java RMI pueden ser vulnerables a ataques de deserialización, lo que permite a un atacante ejecutar código arbitrario en el servidor.
   - **Recomendación**: Asegurar las aplicaciones que utilizan RMI con políticas de seguridad Java y limitar el acceso a estos servicios a redes internas seguras.

Vulnerabilidades Críticas Detectadas

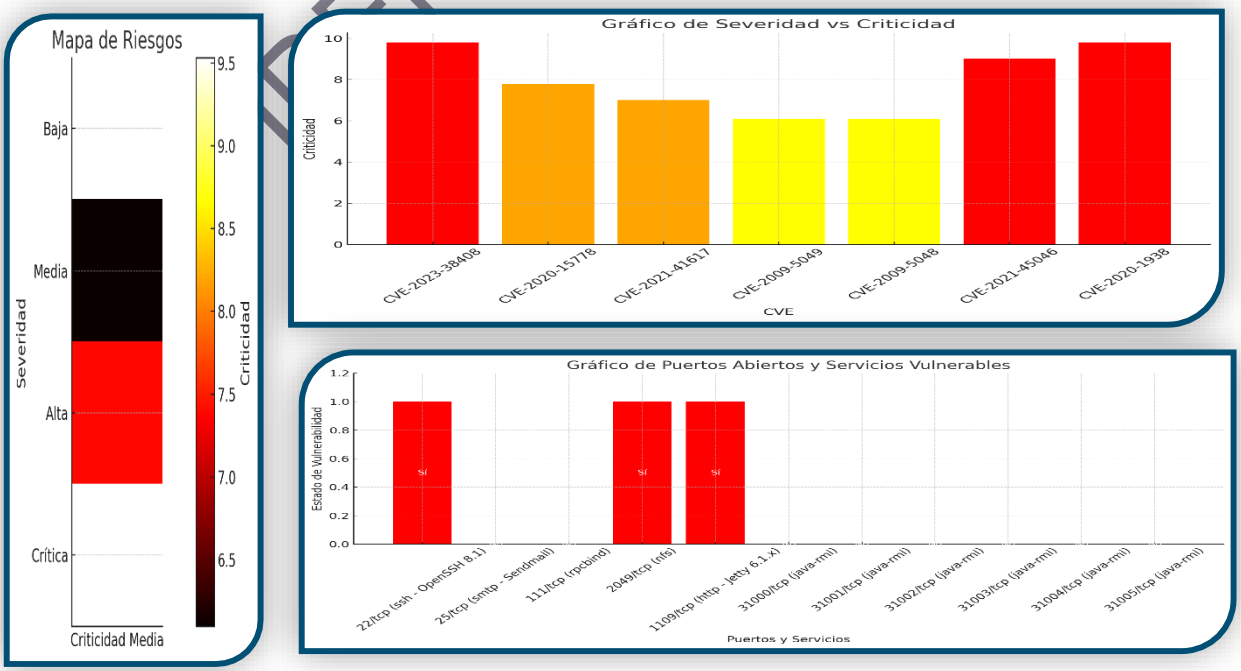
1. **CVE-2023-38408 (SSH Exploit)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en OpenSSH.
   - **Mitigación**: Actualizar OpenSSH y habilitar autenticación de múltiples factores (MFA).
2. **CVE-2009-5049 (Jetty 6.1.x Exploit)** - **Criticidad: 6.1 - Media**
   - **Descripción**: Fuga de información en Jetty 6.1.x.
   - **Mitigación**: Actualizar Jetty a una versión más reciente para prevenir la fuga de información.
3. **CVE-2020-15778 (SSH Exploit)** - **Criticidad: 7.8 - Alta**
   - **Descripción**: Vulnerabilidad que permite la ejecución de comandos arbitrarios en sistemas remotos.
   - **Mitigación**: Aplicar las actualizaciones necesarias a OpenSSH.
4. **CVE-2021-41617 (SSH)** - **Criticidad: 7.0 - Alta**
   - **Descripción**: Vulnerabilidad que permite ataques de denegación de servicio.
   - **Mitigación**: Actualizar OpenSSH y aplicar parches de seguridad.
5. **CVE-2021-45046 (Log4Shell)** - **Criticidad: 9.0 - Crítica**
   - **Descripción**: Vulnerabilidad en Apache Log4j que permite la ejecución remota de código.
   - **Mitigación**: Actualizar Apache Log4j a la versión 2.17 o superior.

6. **CVE-2020-1938 (Ghostcat - Apache Tomcat)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad en Apache Tomcat y su conector AJP que permite la lectura de archivos confidenciales en el servidor.
    - **Mitigación**: Deshabilitar o asegurar el puerto AJP y restringir su acceso a redes internas.

Recomendaciones de Seguridad

- **Actualizar OpenSSH y Jetty**: Dado el número de vulnerabilidades críticas y medias asociadas con OpenSSH y Jetty, es fundamental actualizar estas aplicaciones a las versiones más recientes.
- **Fortalecer la configuración de Sendmail**: Implementar políticas de seguridad como SPF, DKIM y TLS para asegurar el envío de correos electrónicos y evitar que Sendmail se utilice como un relé abierto.
- **Restringir el acceso a NFS y rpcbind**: Asegurarse de que solo las IPs autorizadas tengan acceso a los recursos compartidos mediante NFS. Además, restringir el acceso a rpcbind para evitar posibles ataques a servicios RPC.
- **Revisar las configuraciones de Java RMI**: Dado que Java RMI es propenso a ataques de deserialización, es importante restringir el acceso solo a redes internas seguras y aplicar políticas de seguridad adicionales.
- **Asegurar Apache Tomcat y Log4j**: Actualizar Apache Tomcat y Log4j a las versiones más recientes para mitigar vulnerabilidades críticas como **Ghostcat** y **Log4Shell**.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.120

Puertos Abiertos y Servicios Asociados

1. **13/tcp - daytime**
    - **Descripción**: Servicio que devuelve la fecha y la hora.
    - **Recomendación**: Este servicio es obsoleto y debe deshabilitarse si no es necesario.
2. **21/tcp - ftp (HP-UX o AIX ftpd 4.2)**
    - **Vulnerabilidades**:
        - **CVE-2001-0311** (Criticidad: 4.6 - Media): Ejecución remota de código a través de vulnerabilidades en FTP.
    - **Recomendación**: Deshabilitar FTP y migrar a SFTP o FTPS, que cifran las credenciales y los datos transmitidos. FTP transmite credenciales en texto claro, lo que lo hace vulnerable a ataques de interceptación y ejecución de código.
3. **22/tcp - ssh (OpenSSH 8.1, protocolo 2.0)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución de comandos arbitrarios.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
    - **Recomendación**: Actualizar OpenSSH a la última versión, habilitar autenticación multifactor (MFA) y usar claves SSH en lugar de contraseñas. También es recomendable implementar **Fail2Ban** para mitigar ataques de fuerza bruta.
4. **23/tcp - telnet (AIX telnetd)**
    - **Descripción**: Protocolo Telnet que permite acceso remoto no cifrado.
    - **Recomendación**: Deshabilitar completamente Telnet y reemplazarlo por SSH, ya que Telnet transmite credenciales y datos en texto claro, haciéndolo altamente vulnerable a ataques de intermediarios.
5. **25/tcp - nagios-nsca**
    - **Descripción**: Servicio utilizado para la transmisión de datos del sistema de monitorización Nagios.
    - **Recomendación**: Asegurar este servicio con TLS y limitar el acceso a redes internas.
6. **111/tcp - rpcbind**
    - **Descripción**: Servicio utilizado para asignar direcciones a servicios RPC.
    - **Recomendación**: Limitar el acceso a este puerto a redes internas y utilizar reglas de firewall para controlar el acceso a rpcbind, ya que es un objetivo común de ataques.

7. **2049/tcp** - **nfs (Network File System)**
    - **Descripción**: Sistema de archivos en red que permite compartir archivos entre servidores.
    - **Vulnerabilidades**: Si no está configurado adecuadamente, NFS puede exponer archivos sensibles a usuarios no autorizados.
    - **Recomendación**: Configurar listas de control de acceso (ACL) para limitar el acceso solo a hosts autorizados. Considerar la autenticación con Kerberos para reforzar la seguridad de NFS.
8. **5005/tcp** - **jdwp (Java Debug Wire Protocol)**
    - **Descripción**: Protocolo de depuración de Java utilizado para la depuración remota de aplicaciones Java.
    - **Recomendación**: Deshabilitar JDWP en entornos de producción para evitar la ejecución de código malicioso. Este puerto debe ser utilizado solo en entornos de desarrollo o pruebas internas.
9. **1108/tcp** - **java-rmi**
    - **Descripción**: Servicio de invocación de métodos remotos en Java (RMI).
    - **Vulnerabilidades**: Java RMI es propenso a ataques de deserialización maliciosa si no se configura correctamente.
    - **Recomendación**: Restringir el acceso a Java RMI a redes internas y asegurarse de que esté configurado adecuadamente para evitar ataques.
10. **9081/tcp** - **cisco-aqos**

- **Descripción**: Servicio relacionado con Cisco AQOS (calidad de servicio).
- **Recomendación**: Verificar las configuraciones de este servicio y asegurarse de que no esté expuesto a redes externas sin las medidas de seguridad apropiadas.

Vulnerabilidades Críticas Detectadas

1. **CVE-2023-38408 (SSH Exploit)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Ejecución remota de código a través de SSH.
    - **Mitigación**: Actualizar OpenSSH a la última versión y habilitar MFA.
2. **CVE-2001-0311 (FTP - AIX ftpd)** - **Criticidad: 4.6 - Media**
    - **Descripción**: Ejecución remota de código en el servicio FTP.
    - **Mitigación**: Deshabilitar FTP y migrar a SFTP o FTPS.
3. **CVE-2020-15778 (SSH Exploit)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad que permite la ejecución de comandos arbitrarios en SSH.

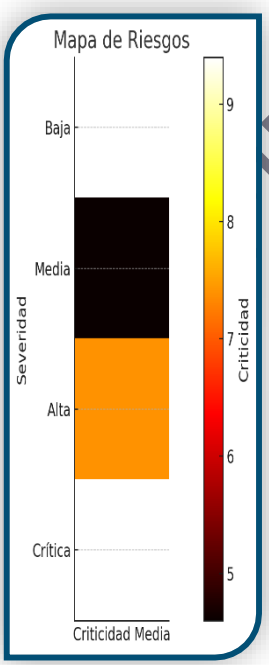
- **Mitigación**: Actualizar OpenSSH y asegurar las políticas de acceso.

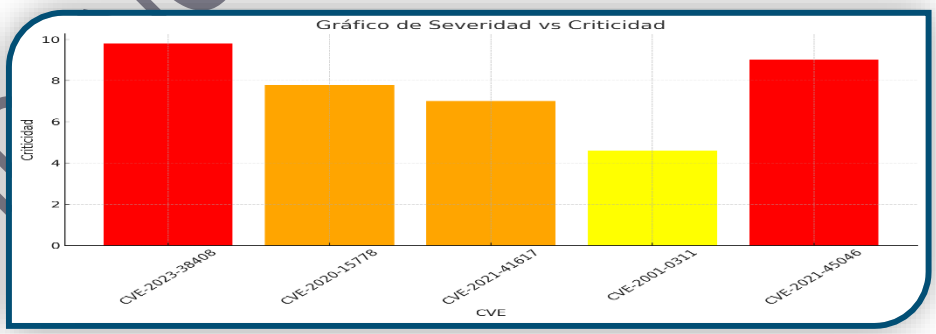
4. **CVE-2021-41617 (SSH)** - **Criticidad: 7.0 - Alta**
   - **Descripción**: Denegación de servicio en OpenSSH.
   - **Mitigación**: Actualizar y aplicar parches a OpenSSH.
5. **CVE-2021-45046 (Log4Shell)** - **Criticidad: 9.0 - Crítica**
   - **Descripción**: Vulnerabilidad en Apache Log4j que permite la ejecución remota de código.
   - **Mitigación**: Actualizar Apache Log4j a la versión 2.17 o superior.

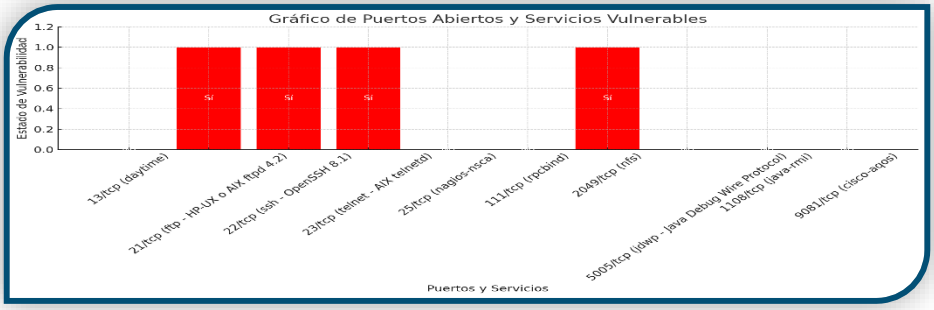
Recomendaciones de Seguridad

- **Deshabilitar FTP y Telnet**: Estos servicios deben deshabilitarse o reemplazarse por alternativas más seguras como SFTP y SSH, ya que transmiten credenciales en texto claro.
- **Asegurar NFS y rpcbind**: Configurar listas de control de acceso para NFS y restringir rpcbind a redes internas.
- **Deshabilitar JDWP en producción**: Este puerto debe estar deshabilitado en entornos de producción para evitar que los atacantes ejecuten código malicioso.
- **Actualizar OpenSSH**: Aplicar parches de seguridad y utilizar MFA para reforzar la seguridad en las conexiones remotas.
- **Revisar y parchear Cisco AQOS**: Asegurarse de que los servicios de calidad de servicio estén configurados adecuadamente para evitar su explotación.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.122

Puertos Abiertos y Servicios Asociados

1. **22/tcp - SSH (OpenSSH 8.7, protocolo 2.0)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
    - **Recomendación**: Actualizar OpenSSH a la última versión, habilitar autenticación multifactor (MFA), usar claves SSH en lugar de contraseñas, e implementar medidas adicionales como **Fail2Ban** para mitigar ataques de fuerza bruta.
2. **443/tcp - Apache Tomcat**
    - **Vulnerabilidades**:
        - **CVE-2020-1938 (Ghostcat)** (Criticidad: 9.8 - Crítica): Ejecución remota de código a través del conector AJP.
        - **CVE-2017-12617** (Criticidad: 7.5 - Alta): Carga arbitraria de archivos que permite la ejecución de código.
    - **Recomendación**: Actualizar Apache Tomcat a la última versión, deshabilitar el conector AJP si no es necesario y aplicar configuraciones de seguridad en el archivo **server.xml** para limitar el acceso no autorizado.
3. **2222/tcp - EtherNetIP-1**
    - **Descripción**: Servicio relacionado con protocolos industriales de control y automatización.
    - **Recomendación**: Limitar el acceso a este puerto a redes seguras y considerar su deshabilitación si no es necesario. Utilizar reglas de firewall para proteger este servicio.
4. **2223/tcp - rockwell-csp2**
    - **Descripción**: Similar a EtherNetIP-1, relacionado con sistemas de control industrial.
    - **Recomendación**: Asegurar que este puerto esté limitado a redes internas, y aplicar reglas de firewall para bloquear accesos no autorizados.
5. **10000/tcp - Webmin**
    - **Descripción**: Servicio Webmin para la administración de servidores.
    - **Vulnerabilidades**: Si está mal configurado, Webmin puede ser vulnerable a ataques de fuerza bruta y ejecución remota de código.
    - **Recomendación**: Limitar el acceso a Webmin a IPs autorizadas y habilitar **HTTPS** para proteger las comunicaciones. Deshabilitar el servicio si no es necesario.

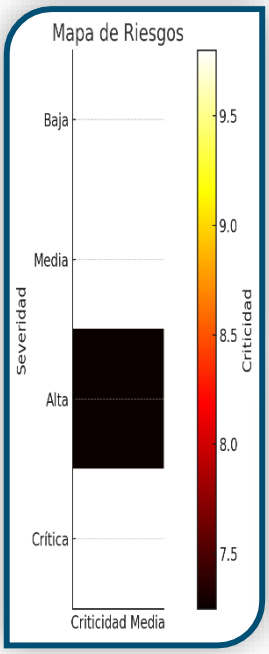
Vulnerabilidades Críticas Detectadas

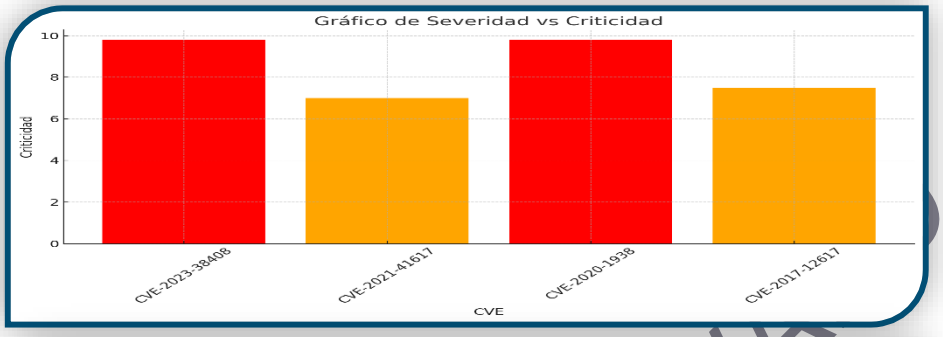
1. **CVE-2023-38408 (SSH Exploit)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Ejecución remota de código a través de SSH.
    - **Mitigación**: Actualizar OpenSSH y habilitar autenticación de múltiples factores (MFA).
2. **CVE-2021-41617 (SSH Exploit)** - **Criticidad: 7.0 - Alta**
    - **Descripción**: Denegación de servicio.
    - **Mitigación**: Aplicar parches de seguridad en SSH y monitorear el uso del servicio.
3. **CVE-2020-1938 (Ghostcat - Apache Tomcat)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad en el conector AJP de Apache Tomcat que permite la lectura de archivos confidenciales o la ejecución remota de código.
    - **Mitigación**: Deshabilitar el conector AJP si no es necesario, o configurarlo de manera segura para restringir el acceso.
4. **CVE-2017-12617 (Apache Tomcat)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en Apache Tomcat que permite la carga arbitraria de archivos, lo que podría llevar a la ejecución de código.
    - **Mitigación**: Actualizar Tomcat a la última versión y asegurar las configuraciones de carga de archivos.

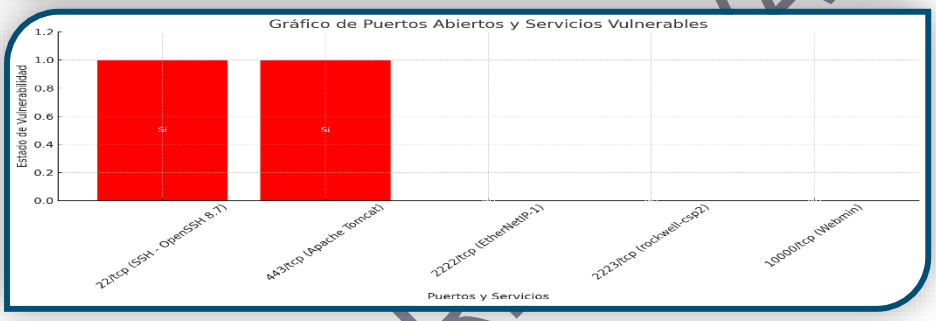
Recomendaciones de Seguridad

- **Fortalecer las políticas de acceso SSH**: Implementar autenticación basada en claves, usar **Fail2Ban** para mitigar intentos de fuerza bruta, y restringir el acceso a redes autorizadas.
- **Actualizar y asegurar Apache Tomcat**: Aplicar las actualizaciones necesarias y limitar el acceso a través de configuraciones de seguridad estrictas, especialmente en el uso del conector AJP.
- **Proteger los servicios en los puertos 2222 y 2223**: Asegurarse de que los servicios relacionados con EtherNetIP-1 y rockwell-csp2 estén limitados a redes internas seguras y protegidos por firewalls.
- **Limitar el acceso a Webmin**: Si Webmin está habilitado, asegurar que solo sea accesible mediante **HTTPS** y restringir el acceso a usuarios confiables.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.126

Puertos Abiertos y Servicios Asociados

1. **80/tcp - HTTP (Apache httpd)**
    - **Descripción**: Servidor HTTP Apache en el puerto 80.
    - **Vulnerabilidades**:
        - Susceptible a ataques de **Cross-Site Scripting (XSS)** y **Directory Traversal** si no está configurado adecuadamente.
    - **Recomendación**: Asegurar que Apache esté configurado con **TLS/SSL**, actualizar a la última versión, y habilitar reglas de seguridad como **ModSecurity**.
2. **135/tcp - MSRPC (Microsoft Windows RPC)**
    - **Descripción**: Servicio de llamadas a procedimientos remotos de Microsoft.
    - **Vulnerabilidades**: Explotado comúnmente en ataques de escalada de privilegios.
    - **Recomendación**: Limitar el acceso a redes internas y autenticar correctamente el servicio RPC.
3. **139/tcp - NetBIOS-SSN (Microsoft Windows NetBIOS-SSN)**
    - **Descripción**: Servicio NetBIOS para compartir archivos y otros recursos en la red.
    - **Recomendación**: Deshabilitar si no es necesario, ya que es un vector común de ataques de malware como **WannaCry**.
4. **445/tcp - Microsoft-DS (Microsoft Windows Server 2008 R2 - 2012)**
    - **Descripción**: Servicio de recursos compartidos en red.
    - **Vulnerabilidades**:
        - Susceptible a ataques de malware como **EternalBlue** y **WannaCry**.
    - **Recomendación**: Deshabilitar o restringir el acceso a redes internas seguras y aplicar configuraciones robustas.
5. **3389/tcp - MS-WBT-Server (Microsoft Terminal Services - RDP)**
    - **Descripción**: Servicio de escritorio remoto.
    - **Vulnerabilidades**:
        - **CVE-2019-0708 (BlueKeep)**: Ejecución remota de código sin autenticación.
    - **Recomendación**: Usar autenticación multifactor (MFA), aplicar parches, y considerar el uso de una **VPN** para conexiones seguras en lugar de exponer el puerto 3389.
6. **4434/tcp - Servicio desconocido**
    - **Descripción**: Puerto 4434 sin identificación clara.

- **Recomendación**: Realizar un análisis de tráfico para identificar el servicio y verificar su necesidad. Limitar el acceso con firewalls si es necesario.

7. **5985/tcp** - **HTTP (Microsoft HTTPAPI httpd 2.0)**
   - **Descripción**: Servidor HTTP usado para la API HTTP de Microsoft.
   - **Recomendación**: Mantener actualizado y configurar para evitar accesos no autorizados.
8. **10050/tcp y 15003/tcp** - **Tcpwrapped**
   - **Descripción**: Servicios protegidos mediante **TCP Wrappers**.
   - **Recomendación**: Verificar las configuraciones de **TCP Wrappers** y asegurar que solo usuarios autorizados puedan acceder.

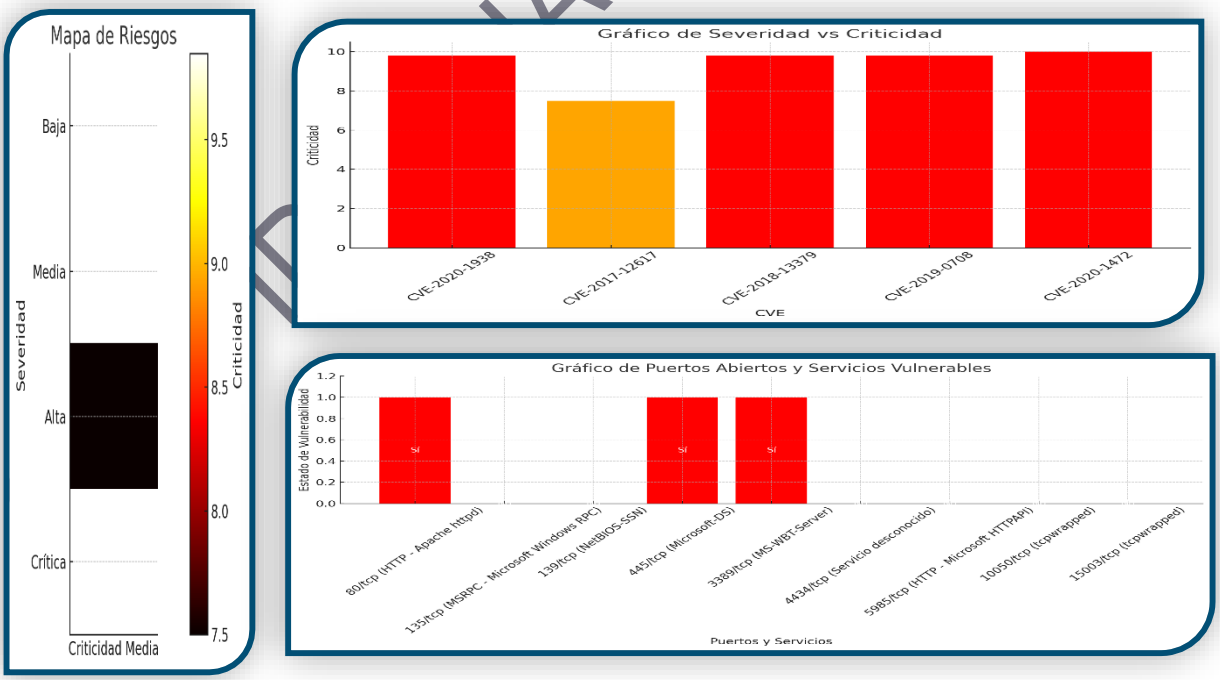
Vulnerabilidades Críticas Detectadas

1. **CVE-2020-1938 (Ghostcat - Apache Tomcat)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en el conector AJP de Apache Tomcat que permite la ejecución remota de código.
   - **Mitigación**: Deshabilitar el conector AJP si no es necesario o restringir su acceso.
2. **CVE-2017-12617 (Apache Tomcat)** - **Criticidad: 7.5 - Alta**
   - **Descripción**: Vulnerabilidad que permite la carga arbitraria de archivos.
   - **Mitigación**: Actualizar Apache Tomcat y reforzar las políticas de seguridad.
3. **CVE-2018-13379 (Fortinet SSL VPN)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en Fortinet SSL VPN que permite la descarga no autenticada de archivos.
   - **Mitigación**: Actualizar Fortinet SSL VPN a la última versión disponible.
4. **CVE-2019-0708 (BlueKeep - Escritorio Remoto)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en el servicio de Escritorio Remoto que permite la ejecución remota de código sin autenticación.
   - **Mitigación**: Aplicar los parches de seguridad de Microsoft para evitar la explotación.
5. **CVE-2020-1472 (Netlogon Privilege Escalation)** - **Criticidad: 10.0 - Crítica**
   - **Descripción**: Vulnerabilidad en Netlogon que permite escalada de privilegios.
   - **Mitigación**: Actualizar y revisar las configuraciones de acceso en los controladores de dominio.

Recomendaciones de Seguridad

- **Asegurar Apache HTTP**: Implementar **TLS/SSL**, aplicar reglas de seguridad como **ModSecurity**, y actualizar Apache a la última versión disponible.
- **Deshabilitar NetBIOS/SMB si no es necesario**: Dado que los puertos 135, 139 y 445 son objetivos comunes para malware como **WannaCry** y **EternalBlue**, se recomienda deshabilitarlos si no son críticos para el entorno.
- **Reforzar RDP (Escritorio Remoto)**: Implementar autenticación multifactor (MFA), parchear **BlueKeep**, y considerar el uso de **VPN** para acceder de forma segura al escritorio remoto.
- **Revisar y proteger servicios desconocidos**: El puerto 4434 debe ser analizado para identificar su uso y asegurarse de que esté protegido adecuadamente.
- **Mantener actualizados todos los servicios críticos**: Asegurarse de que Apache, RDP y otros servicios tengan las actualizaciones más recientes para mitigar vulnerabilidades críticas.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.129

Puertos Abiertos y Servicios Asociados

1. **22/tcp - SSH (OpenSSH 7.9p1 Debian 10+deb10u2, protocolo 2.0)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución remota de comandos.
        - **CVE-2021-41617** (Criticidad: 7.0 - Alta): Denegación de servicio.
    - **Recomendación**: Actualizar OpenSSH a la última versión, aplicar autenticación basada en claves SSH, habilitar MFA y utilizar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta.
2. **80/tcp - HTTP (Apache httpd 2.4.38, Debian)**
    - **Vulnerabilidades**:
        - **CVE-2023-25690** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2021-44790** (Criticidad: 9.8 - Crítica): Inyección de código.
    - **Recomendación**: Actualizar Apache a la última versión disponible, implementar **TLS/SSL**, revisar las configuraciones de seguridad en **httpd.conf** y habilitar módulos como **ModSecurity** para proteger contra vulnerabilidades como **XSS** y **Directory Traversal**.
3. **3000/tcp - Grafana HTTP**
    - **Vulnerabilidades**:
        - **CVE-2021-43798** (Criticidad: 7.5 - Alta): **Directory traversal** que permite leer archivos arbitrarios.
    - **Recomendación**: Actualizar Grafana a la última versión, habilitar **TLS/SSL** y configurar autenticación de múltiples factores (MFA).
4. **3306/tcp - MySQL**
    - **Vulnerabilidades**:
        - **CVE-2020-13379** (Criticidad: 7.8 - Alta): Omisión de autenticación en configuraciones específicas.
    - **Recomendación**: Actualizar MySQL, asegurar que las contraseñas de las bases de datos estén cifradas, y aplicar políticas de seguridad robustas para prevenir acceso no autorizado y ataques de inyección SQL.

5. **10050/tcp y 10051/tcp** - **Zabbix-Agent y Zabbix-Trapper**
    - **Vulnerabilidades**:
        - **CVE-2019-5018** (Criticidad: 7.5 - Alta): Ejecución remota de comandos en Zabbix-Trapper.
    - **Recomendación**: Actualizar Zabbix, restringir el acceso a los servicios solo a direcciones IP autorizadas, y aplicar reglas de firewall para proteger los servicios de monitoreo.
6. **10053/tcp** - **HTTP (Golang net/http server)**
    - **Descripción**: Servicio HTTP basado en Golang, utilizado por **Go-IPFS json-rpc** o **InfluxDB API**.
    - **Recomendación**: Asegurar el servicio mediante **TLS/SSL** y limitar el acceso a redes internas confiables.
7. **33060/tcp** - **MySQLX**
    - **Descripción**: Protocolo MySQL X, utilizado para la comunicación con bases de datos.
    - **Recomendación**: Limitar el acceso a redes internas, habilitar **TLS** para asegurar las conexiones, y verificar las políticas de autenticación.

Vulnerabilidades Críticas Detectadas

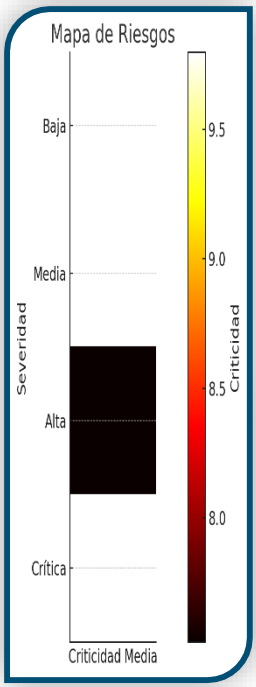
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y restringir el acceso solo a IPs autorizadas.
2. **CVE-2023-25690 (Apache HTTP)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad en Apache HTTP que permite la ejecución remota de código.
    - **Mitigación**: Actualizar Apache y aplicar configuraciones de seguridad adecuadas.
3. **CVE-2021-44790 (Apache HTTP)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Inyección de código en Apache HTTP.
    - **Mitigación**: Actualizar Apache a la última versión disponible y aplicar medidas de seguridad.
4. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad que permite la ejecución de comandos arbitrarios en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y revisar las políticas de acceso y autenticación.

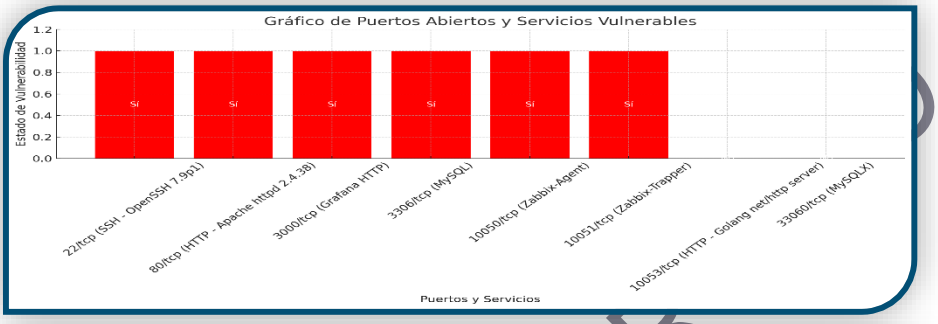
5. **CVE-2021-41617 (OpenSSH)** - **Criticidad: 7.0 - Alta**
    - **Descripción**: Vulnerabilidad de denegación de servicio en OpenSSH.
    - **Mitigación**: Aplicar los parches de seguridad necesarios y ajustar la configuración de seguridad.
6. **CVE-2021-43798 (Grafana)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad que permite ataques de **directory traversal** en Grafana.
    - **Mitigación**: Actualizar Grafana y revisar los permisos de acceso a archivos.
7. **CVE-2020-13379 (MySQL)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad de omisión de autenticación en configuraciones específicas de MySQL.
    - **Mitigación**: Actualizar MySQL y aplicar configuraciones de autenticación seguras.
8. **CVE-2019-5018 (Zabbix)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en Zabbix-Trapper que permite la ejecución remota de comandos.
    - **Mitigación**: Actualizar Zabbix y reforzar las políticas de seguridad.

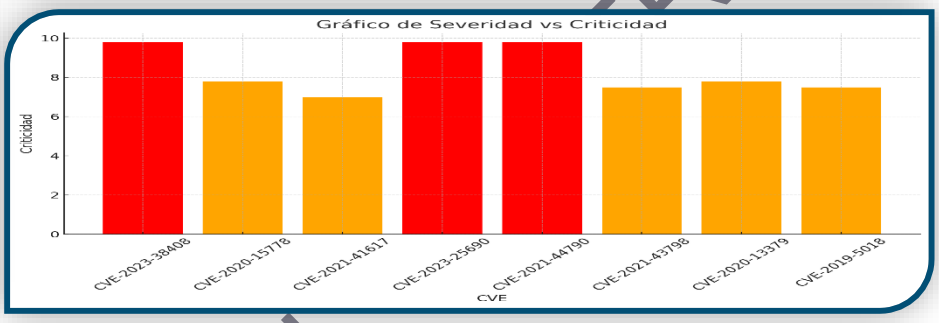
Recomendaciones de Seguridad

- **Actualizar y asegurar OpenSSH**: Implementar medidas de seguridad como la autenticación basada en claves y el uso de **Fail2Ban** para proteger contra ataques de fuerza bruta. Aplicar actualizaciones críticas para prevenir vulnerabilidades de ejecución de código.
- **Fortalecer Apache HTTP**: Actualizar a la última versión de Apache, habilitar **TLS/SSL** para proteger las comunicaciones y aplicar configuraciones de seguridad como **ModSecurity** para mitigar ataques de **XSS** y **directory traversal**.
- **Proteger servicios MySQL y MySQLX**: Asegurarse de que las configuraciones de autenticación de MySQL estén protegidas, aplicar cifrado TLS en las conexiones y limitar el acceso a redes internas confiables.
- **Actualizar Grafana y aplicar autenticación fuerte**: Implementar **TLS/SSL** y autenticación multifactor (MFA) en Grafana para proteger el acceso al panel de control. Asegurarse de que las actualizaciones de seguridad estén aplicadas.
- **Restringir el acceso a los servicios de monitoreo (Zabbix)**: Limitar las conexiones de Zabbix a redes internas autorizadas y aplicar reglas de firewall para proteger los servicios de monitoreo.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.142

Puertos Abiertos y Servicios Asociados

1. **22/tcp - SSH (OpenSSH 9.2p1 Debian)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2023-28531** (Criticidad: 9.8 - Crítica): Vulnerabilidad crítica.
        - **Exploits** disponibles para OpenSSH 9.2p1.
    - **Recomendación**: Actualizar OpenSSH a la última versión, implementar autenticación basada en claves SSH y habilitar MFA para todos los usuarios. Además, usar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta y deshabilitar el acceso root por SSH.
2. **80/tcp - HTTP (OpenResty Web App Server)**
    - **Vulnerabilidades**:
        - **CVE-2023-51385** (Criticidad: 6.5 - Media): Explotación posible si no se asegura adecuadamente.
    - **Recomendación**: Actualizar OpenResty a la última versión y aplicar **TLS/SSL** para proteger las comunicaciones HTTP. Revisar las configuraciones de seguridad en los módulos **Lua** y **Nginx**.
3. **81/tcp - HTTP (OpenResty Web App Server)**
    - **Recomendación**: Verificar la seguridad del servidor y asegurar que esté correctamente actualizado y configurado para evitar ataques de inyección.
4. **443/tcp - HTTPS (OpenResty Web App Server)**
    - **Recomendación**: Asegurar que los certificados **TLS** estén actualizados y correctamente configurados. Utilizar algoritmos de cifrado robustos como **TLS 1.2** o **TLS 1.3** para evitar ataques de interceptación de tráfico.
5. **4100/tcp - HTTP (Apache Tomcat)**
    - **Vulnerabilidades**:
        - **CVE-2020-9484** (Criticidad: 8.1 - Alta): Ejecución de código arbitrario a través de la deserialización de datos.
    - **Recomendación**: Actualizar Apache Tomcat a la última versión, asegurar que el conector **AJP** esté deshabilitado si no es necesario, y aplicar configuraciones de seguridad en **server.xml** para limitar el acceso no autorizado.

6. **5432/tcp** - **PostgreSQL 16.0 - 16.2**
    - **Vulnerabilidades**:
        - **CVE-2019-3466** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite a atacantes ejecutar comandos arbitrarios a través de inyección SQL.
    - **Recomendación**: Actualizar PostgreSQL a la versión más reciente, aplicar autenticación robusta basada en roles y habilitar **SSL** para proteger las conexiones de la base de datos.
7. **9001/tcp** - **HTTP (Golang net/http server)**
    - **Recomendación**: Limitar el acceso a este servicio solo a redes internas confiables y asegurar las comunicaciones mediante **TLS** para proteger los datos en tránsito.

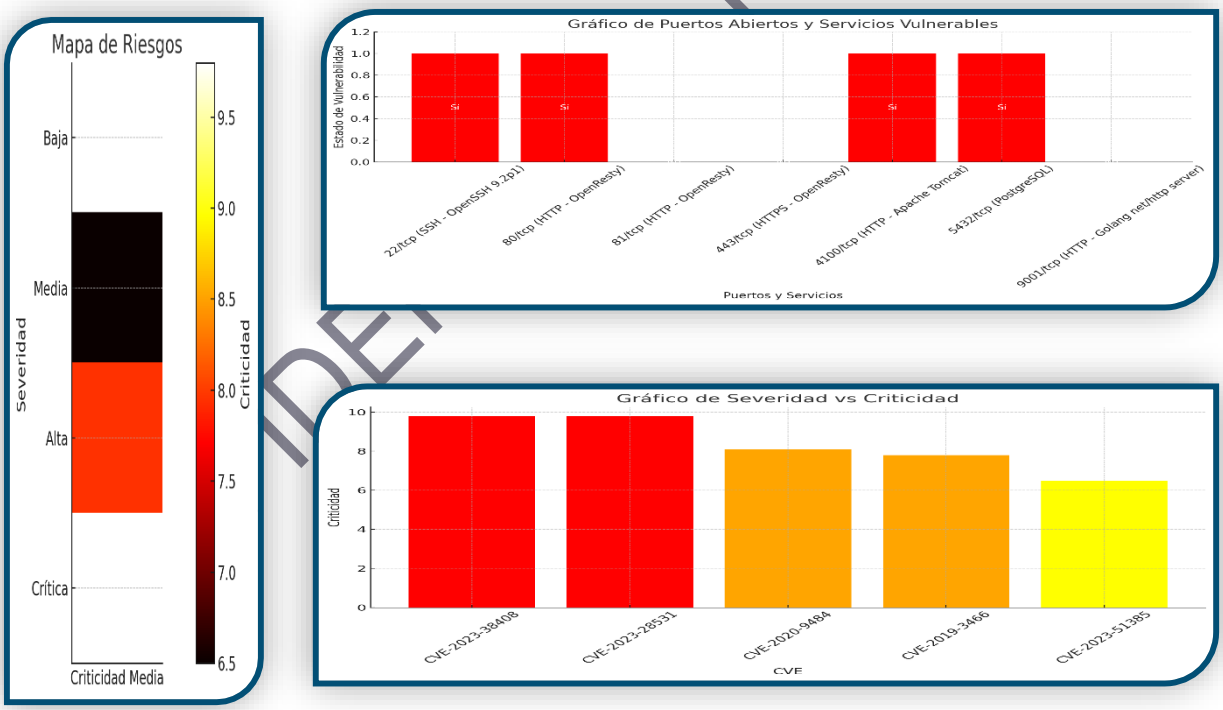
Vulnerabilidades Críticas Detectadas

1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y aplicar autenticación de múltiples factores (MFA).
2. **CVE-2023-28531 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad crítica que afecta versiones anteriores de OpenSSH.
    - **Mitigación**: Aplicar parches de seguridad y limitar el acceso SSH solo a IPs autorizadas.
3. **CVE-2020-9484 (Apache Tomcat)** - **Criticidad: 8.1 - Alta**
    - **Descripción**: Vulnerabilidad en Apache Tomcat que permite la ejecución de código arbitrario mediante deserialización insegura.
    - **Mitigación**: Actualizar Apache Tomcat y revisar las configuraciones del conector AJP y las políticas de serialización.
4. **CVE-2019-3466 (PostgreSQL)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad en PostgreSQL que permite la ejecución de comandos arbitrarios a través de inyección SQL.
    - **Mitigación**: Actualizar PostgreSQL y aplicar políticas de seguridad en la autenticación y consultas SQL.
5. **CVE-2023-51385 (OpenResty)** - **Criticidad: 6.5 - Media**
    - **Descripción**: Explotación posible en servidores OpenResty mal configurados.
    - **Mitigación**: Asegurar que las configuraciones de OpenResty sean óptimas y aplicar actualizaciones de seguridad.

Recomendaciones de Seguridad

- **Actualizar y proteger OpenSSH**: Implementar autenticación basada en claves SSH y **Fail2Ban** para mitigar ataques de fuerza bruta. Aplicar parches de seguridad y asegurar que el acceso root esté deshabilitado.
- **Fortalecer la seguridad de OpenResty**: Asegurar que los certificados **TLS** estén actualizados y habilitar cifrados robustos. Revisar las configuraciones de seguridad en los módulos Lua y Nginx.
- **Proteger Apache Tomcat**: Deshabilitar conectores no utilizados como **AJP** y aplicar las últimas actualizaciones de seguridad para evitar vulnerabilidades como **Remote Code Execution**.
- **Fortalecer la seguridad de PostgreSQL**: Implementar roles de autenticación y aplicar **SSL** en las conexiones de la base de datos para proteger los datos en tránsito.
- **Limitar el acceso a servicios internos**: Asegurar que los servicios HTTP y PostgreSQL estén protegidos mediante firewalls y que el acceso esté restringido solo a redes internas autorizadas.

GRÁFICOS RELEVANTES



Informe Técnico Detallado para IP 172.18.80.155

Puertos Abiertos y Servicios Asociados

1. **13/tcp - Daytime Service**
    - **Descripción**: Servicio que devuelve la fecha y hora actual.
    - **Recomendación**: Este servicio es obsoleto. Si no es necesario, se recomienda deshabilitarlo para reducir la superficie de ataque.
2. **21/tcp - FTP (HP-UX ftpd 4.2)**
    - **Vulnerabilidades**:
        - **CVE-2001-0248** (Criticidad: 7.5 - Alta): Desbordamiento de búfer que permite la ejecución de comandos arbitrarios.
        - **CVE-1999-0961** (Criticidad: 9.0 - Crítica): Permite la obtención de privilegios root.
    - **Recomendación**: Deshabilitar el servicio FTP y reemplazarlo por **SFTP** o **FTPS** que cifran los datos transmitidos.
3. **22/tcp - SSH (OpenSSH 8.1)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución remota de comandos.
    - **Recomendación**: Actualizar OpenSSH a la última versión disponible, habilitar autenticación basada en claves SSH y utilizar **Fail2Ban** para protegerse contra ataques de fuerza bruta.
4. **23/tcp - Telnet (AIX telnetd)**
    - **Descripción**: Protocolo de comunicación remota no cifrado.
    - **Recomendación**: **Telnet** debe ser deshabilitado y reemplazado por **SSH**, ya que transmite credenciales en texto claro.
5. **25/tcp - Nagios NSCA**
    - **Descripción**: Servicio de monitorización usado por **Nagios** para transmitir datos.
    - **Recomendación**: Limitar el acceso a este puerto y protegerlo con TLS para asegurar las comunicaciones.
6. **37/tcp - Time Service (RFC 868)**
    - **Descripción**: Protocolo para sincronización de tiempo.
    - **Recomendación**: Este servicio es obsoleto. Considerar deshabilitarlo o reemplazarlo por **NTP** para sincronización de tiempo segura.

7. **111/tcp** - **RPCBIND**
    - **Vulnerabilidades**:
        - **CVE-1999-0688** (Criticidad: 7.5 - Alta): Desbordamiento de búfer en la función **RPC** que puede ser explotado para ejecutar código arbitrario.
    - **Recomendación**: Actualizar el servicio RPCBIND y limitar su acceso solo a redes internas a través de reglas de firewall.
8. **199/tcp** - **SMUX**
    - **Descripción**: Servicio **Simplex Multiplexing**.
    - **Recomendación**: Si no es necesario, deshabilitar el servicio para reducir la superficie de ataque.
9. **543/tcp** - **klogin (AIX Kerberized rlogin)**
    - **Descripción**: Protocolo de inicio de sesión remoto con autenticación basada en **Kerberos**.
    - **Recomendación**: Asegurarse de que la autenticación **Kerberos** esté correctamente configurada y restringir el acceso solo a redes internas.
10. **544/tcp** - **kshell (AIX Kerberized rshd)**

- **Descripción**: Servicio de shell remoto con autenticación **Kerberos**.
- **Recomendación**: Si no es necesario, deshabilitar el servicio o asegurar que esté configurado correctamente.

11. **32768/tcp** - **filenet-tms**

- **Descripción**: Servicio relacionado con **RPC**.
- **Recomendación**: Limitar el acceso a este puerto mediante firewall.

12. **32769/tcp** - **nlockmgr**

- **Descripción**: Servicio de bloqueo de archivos distribuido.
- **Recomendación**: Asegurar el servicio y limitar el acceso a redes internas.

Vulnerabilidades Críticas Detectadas

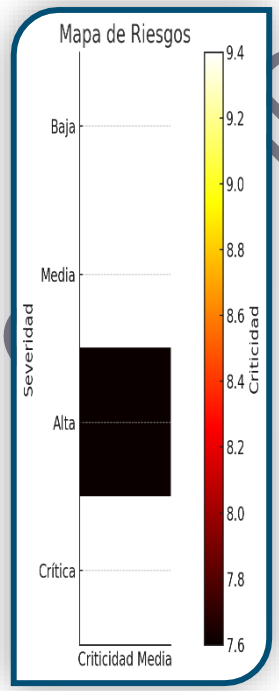
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Ejecución remota de código a través de OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y configurar autenticación basada en claves y multifactor.
2. **CVE-2001-0248 (FTP HP-UX)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Desbordamiento de búfer que permite la ejecución de código arbitrario en servidores FTP.
    - **Mitigación**: Actualizar el servidor FTP o reemplazarlo por SFTP o FTPS.

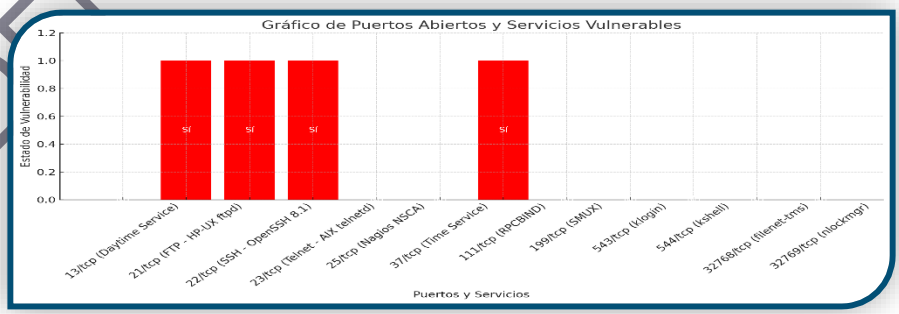
3. **CVE-2020-15778 (SSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Ejecución de comandos arbitrarios en **SSH** a través de desbordamientos de búfer.
    - **Mitigación**: Actualizar OpenSSH a la última versión y reforzar las políticas de autenticación.
4. **CVE-1999-0688 (RPC)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Desbordamiento de búfer en **RPCBIND** que permite la ejecución de código malicioso.
    - **Mitigación**: Actualizar el servicio **RPCBIND** y restringir el acceso a través de reglas de firewall.

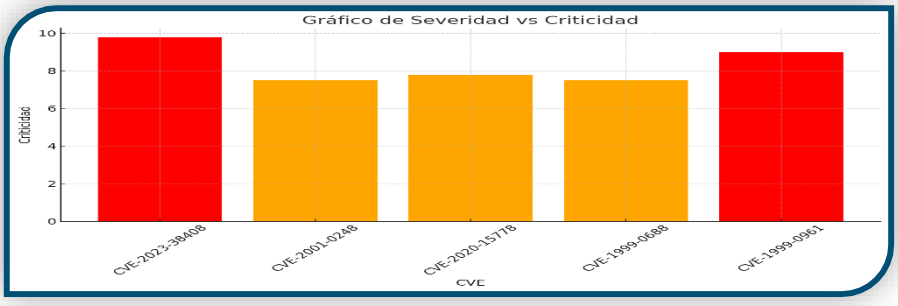
Recomendaciones de Seguridad

- **Deshabilitar servicios obsoletos**: Se recomienda deshabilitar servicios obsoletos como **Telnet**, **Daytime**, **Time** y **FTP** en favor de alternativas más seguras como **SSH**, **SFTP** o **NTP**.
- **Limitar el acceso a servicios sensibles**: Servicios como **RPCBIND**, **klogin**, **kshell** y **nlockmgr** deben estar protegidos mediante reglas de firewall que limiten su acceso solo a redes internas.
- **Actualizar y asegurar OpenSSH**: Aplicar los parches de seguridad más recientes y utilizar autenticación basada en claves SSH, junto con **Fail2Ban** para mitigar ataques de fuerza bruta.
- **Asegurar la sincronización de tiempo**: Reemplazar el protocolo **Time** por **NTP**, que es más seguro y permite una mejor sincronización de tiempo en las redes.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.226

Puertos Abiertos y Servicios Asociados

1. **80/tcp - HTTP (Microsoft IIS httpd 10.0)**
    - **Vulnerabilidades**:
        - **IIS** puede ser susceptible a ataques de **Cross-Site Scripting (XSS)** y **Directory Traversal** si no está configurado adecuadamente.
    - **Recomendación**: Actualizar IIS a la última versión y asegurarse de que las configuraciones de seguridad en **web.config** sean correctas. Implementar **TLS/SSL** para asegurar las comunicaciones.
2. **135/tcp - MSRPC (Microsoft Windows RPC)**
    - **Vulnerabilidades**:
        - **MSRPC** es un objetivo frecuente de ataques de **desbordamiento de búfer** y **DDoS**.
    - **Recomendación**: Limitar el acceso al servicio **MSRPC** solo a usuarios y redes autorizadas. Aplicar los últimos parches de seguridad de Microsoft.
3. **139/tcp y 445/tcp - NetBIOS-ssn y Microsoft-DS (SMB)**
    - **Vulnerabilidades**:
        - Estos puertos están relacionados con **SMB**, que ha sido explotado en ataques como **EternalBlue** y **WannaCry**.
    - **Recomendación**: Deshabilitar SMB desde redes externas y asegurar que solo se utilice **SMBv3**. Aplicar parches de seguridad y proteger el acceso con reglas de firewall.
4. **1433/tcp - MS-SQL-S (Microsoft SQL Server 2012)**
    - **Vulnerabilidades**:
        - **CVE-2023-21713** (Criticidad: 9.8 - Crítica): Vulnerabilidad que permite la ejecución remota de código en SQL Server.
        - **CVE-2020-0618** (Criticidad: 8.8 - Alta): Vulnerabilidad que permite la ejecución remota de código en SQL Server.
    - **Recomendación**: Actualizar **SQL Server** a la versión más reciente, asegurar que se utilice autenticación fuerte y que las comunicaciones estén cifradas.
5. **3389/tcp - MS-WBT-Server (Microsoft Terminal Services - RDP)**
    - **Vulnerabilidades**:
        - **CVE-2019-0708 (BlueKeep)** (Criticidad: 9.8 - Crítica): Permite la ejecución remota de código sin autenticación en RDP.

- **Recomendación**: Limitar el acceso a RDP mediante **VPN**, aplicar **autenticación multifactor (MFA)** y asegurar que los parches contra **BlueKeep** estén aplicados.

6. **5985/tcp - HTTP (Microsoft HTTPAPI httpd 2.0, SSDP/UPnP)**
   - **Vulnerabilidades**:
     - Este puerto es usado para administración remota mediante **WinRM**, lo que lo convierte en un objetivo para ataques si no está protegido adecuadamente.
   - **Recomendación**: Configurar **WinRM** para redes internas solamente, y asegurarse de que **HTTPS** esté habilitado para las comunicaciones.
7. **10050/tcp - Zabbix Agent**
   - **Vulnerabilidades**:
     - Si no se configura adecuadamente, el agente de **Zabbix** puede ser vulnerable a ataques de ejecución remota de comandos.
   - **Recomendación**: Limitar el acceso al agente Zabbix solo a IPs autorizadas y configurar reglas de firewall para proteger el servicio.

Vulnerabilidades Críticas Detectadas

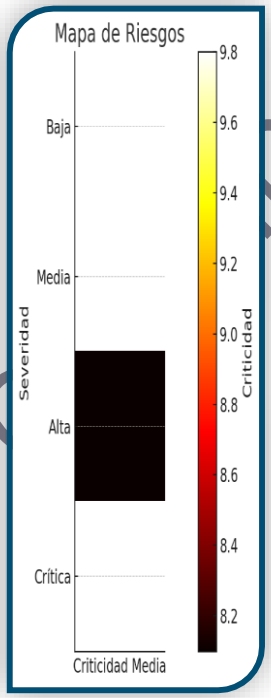
1. **CVE-2023-21713 (Microsoft SQL Server) - Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en Microsoft SQL Server.
   - **Mitigación**: Aplicar inmediatamente las actualizaciones de seguridad de SQL Server.
2. **CVE-2020-0618 (Microsoft SQL Server) - Criticidad: 8.8 - Alta**
   - **Descripción**: Vulnerabilidad en SQL Server que permite la ejecución remota de código a través de consultas maliciosas.
   - **Mitigación**: Asegurarse de que SQL Server esté parcheado y aplicar configuraciones seguras de acceso.
3. **CVE-2019-0708 (BlueKeep - RDP) - Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad en **RDP** que permite la ejecución remota de código sin necesidad de autenticación.
   - **Mitigación**: Aplicar parches de seguridad y limitar el acceso remoto mediante MFA y conexiones a través de VPN.
4. **CVE-2023-21705 y CVE-2021-1636 (Microsoft SQL Server) - Criticidad: Alta**
   - **Descripción**: Vulnerabilidades en SQL Server que permiten la ejecución de código remoto.

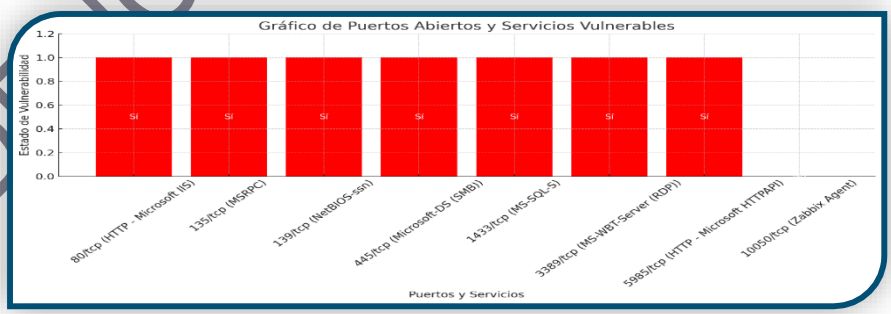
- **Mitigación**: Aplicar actualizaciones de seguridad y asegurar que las políticas de autenticación y permisos en SQL Server sean robustas.

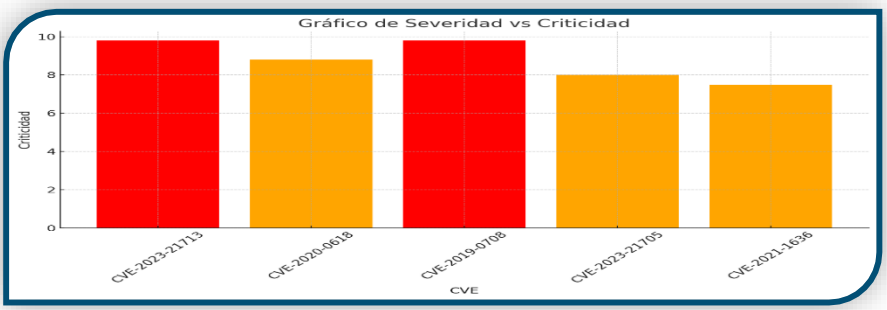
Recomendaciones de Seguridad

- **Actualizar SQL Server y aplicar parches críticos**: Asegurarse de que todas las vulnerabilidades conocidas en **SQL Server** estén parcheadas y aplicar configuraciones de seguridad robustas para mitigar los riesgos de ejecución remota de código.
- **Revisar la configuración de SMB**: Deshabilitar el acceso a **SMB** desde redes externas y asegurarse de que solo se utilice la versión **SMBv3**. Implementar reglas de firewall para proteger estos servicios.
- **Fortalecer la seguridad en IIS**: Implementar políticas de seguridad en **IIS**, incluyendo el uso de **TLS/SSL** y la correcta configuración del archivo **web.config** para prevenir ataques como **XSS** y **Directory Traversal**.
- **Proteger el acceso RDP**: Aplicar autenticación multifactor (MFA), limitar el acceso a **RDP** mediante VPN, y asegurar que todos los parches de seguridad relacionados con **RDP** estén aplicados, especialmente los relacionados con **BlueKeep**.
- **Limitar el acceso a servicios de administración remota (WinRM)**: Asegurar que el acceso a **WinRM** esté restringido solo a redes internas autorizadas y habilitar **HTTPS** para todas las comunicaciones remotas.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 172.18.80.228

Puertos Abiertos y Servicios Asociados

1. **22/tcp - SSH (OpenSSH 8.4p1 Debian)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código en versiones afectadas de OpenSSH.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite la ejecución remota de comandos.
    - **Recomendación**: Actualizar OpenSSH a la última versión disponible. Implementar autenticación basada en claves SSH, deshabilitar el acceso root, y utilizar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta.
2. **80/tcp - HTTP (Apache httpd 2.4.56 - Debian)**
    - **Vulnerabilidades**:
        - **CVE-2023-43622** (Criticidad: 7.5 - Alta): Vulnerabilidad de desbordamiento de búfer que permite la ejecución remota de código.
        - **CVE-2021-44790** (Criticidad: 9.8 - Crítica): Vulnerabilidad de inyección de código.
    - **Recomendación**: Actualizar Apache a la última versión y asegurarse de que las configuraciones de seguridad estén correctamente implementadas, incluyendo el uso de **TLS/SSL** y módulos de protección como **ModSecurity** para prevenir ataques como **XSS** y **Directory Traversal**.
3. **3000/tcp - HTTP (Golang net/http server)**
    - **Descripción**: Servicio HTTP basado en Golang, utilizado por interfaces web o servicios de administración. Puede ser un objetivo de ataques si no está correctamente asegurado.
    - **Recomendación**: Configurar políticas de acceso y autenticación robustas, habilitar **HTTPS** para cifrar las comunicaciones y limitar el acceso solo a redes internas confiables.
4. **10050/tcp - tcpwrapped (Zabbix Agent)**
    - **Descripción**: El puerto **10050** está relacionado con **Zabbix Agent**, utilizado para monitoreo remoto. Si no se configura adecuadamente, puede ser vulnerable a ataques de ejecución remota.
    - **Recomendación**: Limitar el acceso a este puerto mediante reglas de firewall, permitiendo únicamente conexiones desde IPs autorizadas. Habilitar cifrado en las comunicaciones entre el agente Zabbix y el servidor para proteger los datos transmitidos.

Vulnerabilidades Críticas Detectadas

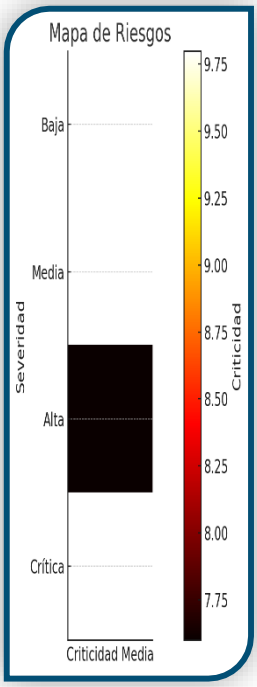
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código a través de OpenSSH.
    - **Mitigación**: Actualizar OpenSSH, aplicar autenticación basada en claves y restringir el acceso solo a IPs autorizadas.
2. **CVE-2023-43622 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en Apache que permite la ejecución remota de código mediante un desbordamiento de búfer.
    - **Mitigación**: Actualizar Apache y aplicar políticas de seguridad estrictas, como la correcta configuración de **TLS/SSL** y **ModSecurity** para mitigar posibles ataques.
3. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de comandos en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y revisar las configuraciones de acceso para prevenir accesos no autorizados.
4. **CVE-2021-44790 (Apache HTTP Server)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad de inyección de código en Apache, que permite a los atacantes ejecutar código arbitrario.
    - **Mitigación**: Aplicar actualizaciones de seguridad y reforzar las políticas de acceso.
5. **CVE-2020-26116 (Golang net/http)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en la implementación HTTP de **Golang**, que permite desbordamientos de búfer.
    - **Mitigación**: Actualizar el servidor HTTP en Golang y aplicar medidas de seguridad adicionales para proteger el acceso.

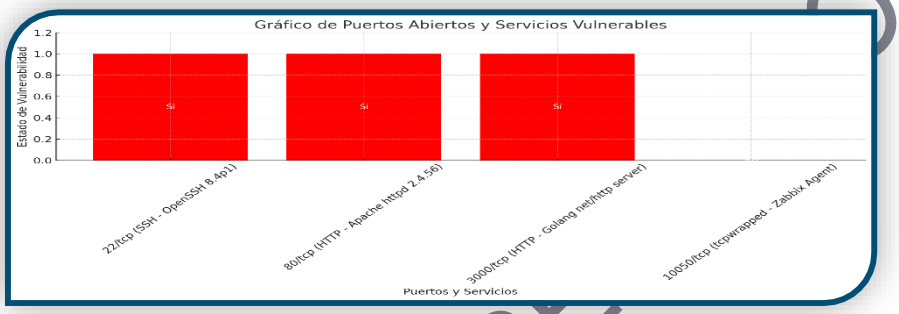
Recomendaciones de Seguridad

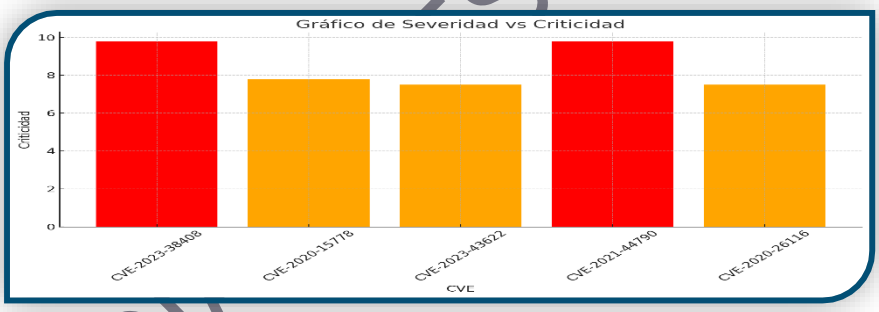
- **Actualizar OpenSSH y Apache**: Es fundamental aplicar parches y actualizaciones para mitigar las vulnerabilidades críticas encontradas en **OpenSSH** y **Apache HTTP Server**.
- **Fortalecer el acceso SSH**: Implementar autenticación basada en claves SSH, deshabilitar el acceso root y utilizar **Fail2Ban** para mitigar ataques de fuerza bruta.
- **Configurar y proteger los servicios HTTP en Golang**: Asegurar que el puerto **3000** solo sea accesible desde redes autorizadas, aplicar autenticación fuerte y habilitar **HTTPS** para cifrar las comunicaciones.

- **Limitar el acceso a Zabbix Agent**: Asegurarse de que el puerto **10050** solo esté disponible para IPs autorizadas y habilitar el cifrado en las comunicaciones entre el agente y el servidor.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 192.168.50.10

Puertos Abiertos y Servicios Asociados

1. **13/tcp - Daytime Service**
    - **Descripción**: Servicio obsoleto que devuelve la fecha y hora actual.
    - **Recomendación**: Deshabilitar este servicio si no es necesario, ya que es obsoleto y aumenta la superficie de ataque.
2. **22/tcp - SSH (OpenSSH 8.1)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Ejecución remota de comandos.
    - **Recomendación**: Actualizar OpenSSH a la última versión. Implementar autenticación basada en claves SSH, deshabilitar el acceso root, y usar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta.
3. **25/tcp - SMTP (Sendmail)**
    - **Descripción**: Servicio de correo electrónico que envía correos a través de **SMTP**.
    - **Recomendación**: Asegurar que **Sendmail** esté configurado para evitar ser utilizado como **open relay**. Implementar autenticación en el envío de correos y aplicar las mejores prácticas de seguridad.
4. **37/tcp - Time Service**
    - **Descripción**: Protocolo para sincronización de hora.
    - **Recomendación**: Reemplazar por **NTP** o deshabilitar si no es necesario, ya que es un servicio obsoleto y vulnerable.
5. **80/tcp - HTTP (IBM HTTP Server derivado de Apache)**
    - **Vulnerabilidades**:
        - **CVE-2020-11979** (Criticidad: 7.5 - Alta): Vulnerabilidad de ejecución remota de código.
        - **CVE-2020-17523** (Criticidad: 8.1 - Alta): Ejecución remota de código en Apache Tomcat.
    - **Recomendación**: Asegurar que el servidor HTTP esté actualizado y que las configuraciones de seguridad estén implementadas, incluyendo el uso de **TLS/SSL** y módulos de protección como **ModSecurity** para prevenir ataques.

6. **111/tcp** - **RPCbind**
    - **Descripción**: Servicio para la gestión de llamadas remotas de procedimiento (RPC).
    - **Recomendación**: Limitar el acceso a **RPCbind** solo a redes internas, actualizar a la última versión y aplicar políticas de seguridad en las configuraciones de red.
7. **199/tcp** - **SMUX**
    - **Descripción**: Protocolo de multiplexación (Simplex Multiplexing).
    - **Recomendación**: Deshabilitar este servicio si no es necesario o protegerlo con reglas de acceso estrictas.
8. **514/tcp** - **tcpwrapped**
    - **Descripción**: El puerto está envuelto por un servicio TCP que controla las conexiones.
    - **Recomendación**: Revisar los servicios detrás de **tcpwrapped** y asegurar que estén protegidos mediante firewalls y autenticación fuerte.
9. **1150/tcp, 1160/tcp, 2006/tcp, 2009/tcp, 50000-50020/tcp, 60000-60020/tcp** - **Java RMI**
    - **Descripción**: Servicios de invocación remota de métodos (Remote Method Invocation) de Java.
    - **Recomendación**: Asegurar que las configuraciones de **Java RMI** incluyan autenticación y cifrado, y limitar el acceso solo a redes internas.
10. **32768-32770/tcp** - **nlockmgr, filenet-tms**
    - **Descripción**: Servicios relacionados con la gestión de bloqueos y administración de archivos a través de RPC.
    - **Recomendación**: Limitar el acceso mediante reglas de firewall y aplicar las actualizaciones de seguridad más recientes.

Vulnerabilidades Críticas Detectadas

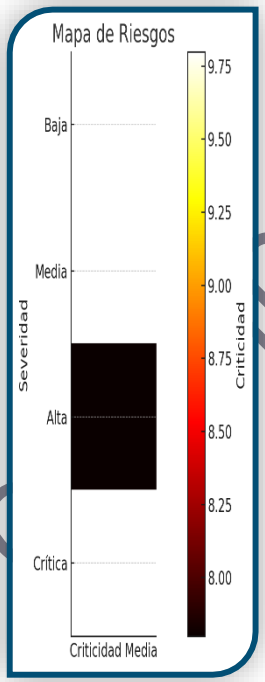
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad de ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y aplicar autenticación basada en claves SSH.
2. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Ejecución de comandos remotos en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y revisar las configuraciones de acceso.
3. **CVE-2020-11979 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad de ejecución remota de código en Apache.
    - **Mitigación**: Actualizar IBM HTTP Server derivado de Apache y configurar las políticas de seguridad correctamente.

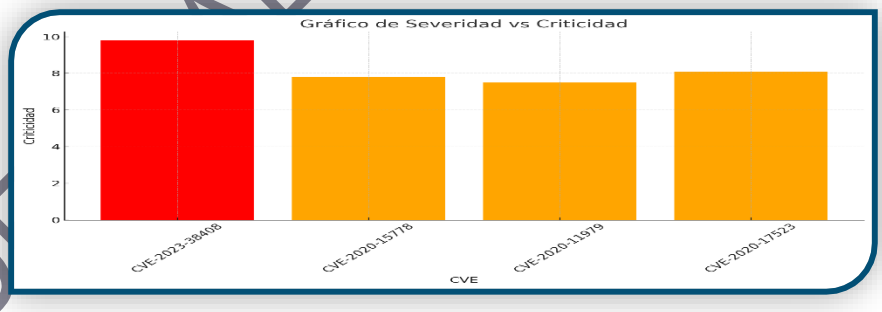
4. **CVE-2020-17523 (Apache Tomcat)** - **Criticidad: 8.1 - Alta**
    - **Descripción**: Ejecución remota de código en Apache Tomcat.
    - **Mitigación**: Aplicar actualizaciones de seguridad y revisar las configuraciones de acceso a **Tomcat**.

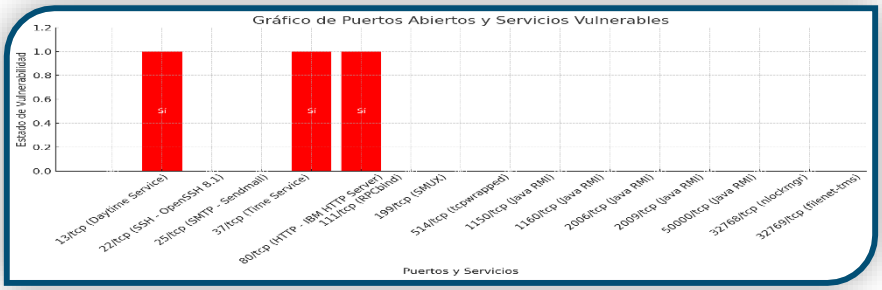
Recomendaciones de Seguridad

- **Actualizar OpenSSH y Sendmail**: Aplicar las actualizaciones y configuraciones necesarias para mitigar vulnerabilidades críticas en **SSH** y **Sendmail**.
- **Deshabilitar servicios obsoletos**: Desactivar servicios como **Daytime** y **Time**, que no son necesarios en entornos modernos y representan un riesgo.
- **Revisar la configuración de IBM HTTP Server**: Asegurarse de que se apliquen las actualizaciones y configuraciones de seguridad necesarias para mitigar ataques como **Cross-Site Scripting (XSS)** y **SQL Injection**.
- **Limitar el acceso a Java RMI y RPCbind**: Restringir el acceso a estos servicios solo a redes internas confiables y aplicar configuraciones de seguridad adicionales para proteger las comunicaciones.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 192.168.50.12

Puertos Abiertos y Servicios Asociados

1. **13/tcp - Daytime Service**
    - **Descripción**: Servicio obsoleto que devuelve la fecha y hora actual.
    - **Recomendación**: Deshabilitar este servicio si no es necesario, ya que es obsoleto y puede representar un riesgo de seguridad.
2. **21/tcp - FTP (HP-UX o AIX ftpd 4.2)**
    - **Vulnerabilidades**:
        - **CVE-2001-0311** (Criticidad: 4.6 - Media): Vulnerabilidad explotable en ftpd.
    - **Recomendación**: Actualizar a una versión más segura o reemplazar **FTP** por **SFTP** o **FTPS** para proteger las credenciales y datos transmitidos.
3. **22/tcp - SSH (OpenSSH 8.1)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite la ejecución remota de comandos.
    - **Recomendación**: Actualizar OpenSSH a la última versión, implementar autenticación basada en claves SSH, deshabilitar el acceso root y utilizar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta.
4. **23/tcp - Telnet (AIX telnetd)**
    - **Descripción**: Telnet transmite datos en texto claro, lo que lo hace vulnerable a ataques de intercepción.
    - **Recomendación**: Deshabilitar **Telnet** y usar **SSH** como alternativa segura para conexiones remotas.
5. **25/tcp - Nagios NSCA**
    - **Descripción**: Servicio para la notificación de alertas de monitoreo.
    - **Recomendación**: Asegurar que las configuraciones sean seguras y restringir el acceso a redes internas de confianza.
6. **37/tcp - Time Service**
    - **Descripción**: Servicio utilizado para la sincronización de tiempo.
    - **Recomendación**: Deshabilitar o reemplazar por **NTP**, ya que este servicio es obsoleto y representa un riesgo de seguridad.

7. **80/tcp - HTTP (IBM HTTP Server)**
    - **Descripción**: Redirige a HTTPS.
    - **Vulnerabilidades**:
        - **CVE-2020-11979** (Criticidad: 7.5 - Alta): Ejecución remota de código en **Apache HTTP Server**.
        - **CVE-2020-17523** (Criticidad: 8.1 - Alta): Vulnerabilidad de ejecución remota en **Apache Tomcat**.
    - **Recomendación**: Actualizar el servidor HTTP, habilitar **TLS/SSL** y asegurar las configuraciones de seguridad en **httpd.conf** y **.htaccess**.
8. **111/tcp - RPCbind**
    - **Descripción**: Servicio utilizado para la gestión de llamadas de procedimiento remoto.
    - **Recomendación**: Limitar el acceso a **RPCbind** solo a redes internas y aplicar parches de seguridad para protegerlo contra ataques de denegación de servicio y desbordamiento de búfer.
9. **199/tcp - SMUX**
    - **Descripción**: Servicio utilizado para multiplexación de conexiones.
    - **Recomendación**: Deshabilitar el servicio si no es necesario o protegerlo mediante políticas de acceso restringido.
10. **443/tcp - HTTPS (Apache HTTP Server 2.4.59)**
    - **Vulnerabilidades**:
        - **CVE-2024-38476** (Criticidad: 9.8 - Crítica): Vulnerabilidad de ejecución remota de código en **Apache HTTP Server**.
        - **CVE-2024-38474** (Criticidad: 9.8 - Crítica): Otra vulnerabilidad crítica en **Apache**.
    - **Recomendación**: Actualizar **Apache HTTP Server** a la versión más reciente y asegurarse de que las configuraciones de **TLS/SSL** estén implementadas adecuadamente para prevenir la explotación de estas vulnerabilidades.
11. **1200/tcp, 21000-21010/tcp - Java RMI**
    - **Descripción**: Servicios relacionados con la invocación remota de métodos en Java.
    - **Recomendación**: Limitar el acceso a estos puertos y aplicar autenticación y cifrado para proteger las comunicaciones.

12. **32768/tcp, 32769/tcp** - **Filenet-tms y nlockmgr**
    - **Descripción**: Servicios relacionados con la gestión de archivos y bloqueos.
    - **Recomendación**: Proteger estos puertos mediante reglas de firewall y aplicar las actualizaciones de seguridad para mitigar vulnerabilidades conocidas.

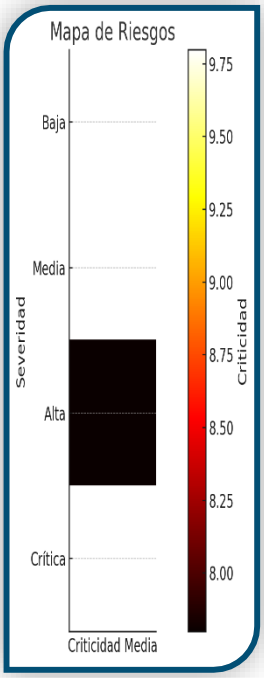
Vulnerabilidades Críticas Detectadas

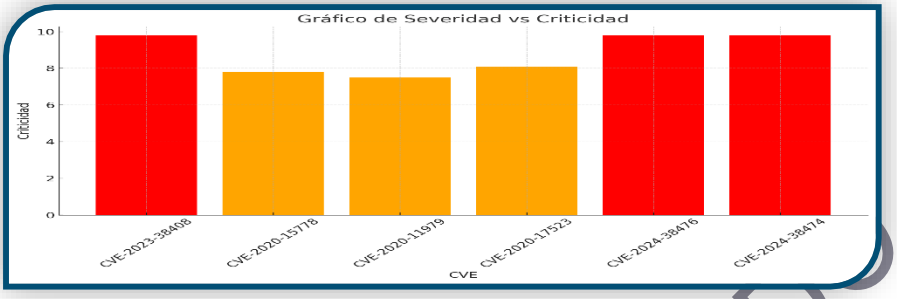
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad de ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH y reforzar las configuraciones de acceso.
2. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Ejecución remota de comandos en OpenSSH.
    - **Mitigación**: Aplicar actualizaciones de seguridad y limitar el acceso SSH a redes confiables.
3. **CVE-2020-11979 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad de ejecución remota de código en Apache HTTP Server.
    - **Mitigación**: Actualizar el servidor HTTP a la última versión y aplicar las mejores prácticas de seguridad.
4. **CVE-2020-17523 (Apache Tomcat)** - **Criticidad: 8.1 - Alta**
    - **Descripción**: Vulnerabilidad de ejecución remota de código en Apache Tomcat.
    - **Mitigación**: Actualizar Apache Tomcat y reforzar las configuraciones de seguridad para prevenir ataques.

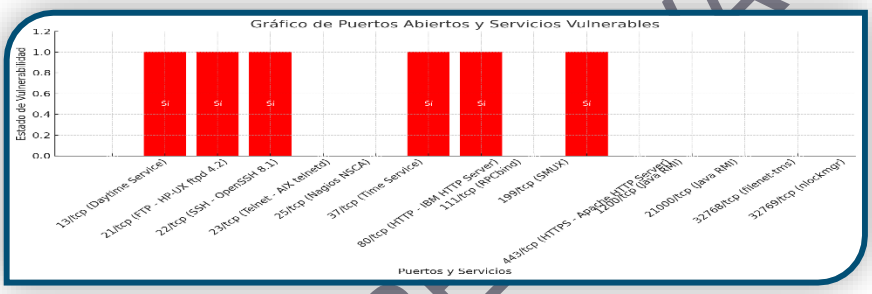
Recomendaciones de Seguridad

- **Actualizar FTP, OpenSSH y Apache HTTP Server**: Aplicar los parches de seguridad más recientes para mitigar vulnerabilidades críticas.
- **Deshabilitar servicios obsoletos**: Desactivar **Telnet**, **Daytime**, y **Time** si no son necesarios en el entorno, ya que representan un riesgo significativo.
- **Proteger Java RMI y RPCbind**: Limitar el acceso a redes internas confiables y aplicar configuraciones de seguridad robustas para proteger los servicios de Java RMI y RPCbind.
- **Reforzar la seguridad de los servicios web**: Implementar **TLS/SSL** correctamente y proteger el acceso mediante autenticación fuerte, asegurando que todas las configuraciones de seguridad estén actualizadas.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para IP 192.168.50.14

Puertos Abiertos y Servicios Asociados

1. **22/tcp (SSH - OpenSSH 8.1)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Vulnerabilidad crítica de ejecución remota de código en OpenSSH.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite la ejecución remota de comandos mediante sftp.
        - **CVE-2021-41617** (Criticidad: 5.8 - Media): Vulnerabilidad que permite a un atacante local obtener privilegios elevados.
    - **Recomendación**: Actualizar OpenSSH a la versión más reciente, implementar autenticación basada en claves SSH, deshabilitar el acceso root y utilizar herramientas como **Fail2Ban** para prevenir ataques de fuerza bruta. Además, restringir el acceso a sftp a usuarios confiables.
2. **80/tcp (HTTP - IBM HTTP Server)**
    - **Descripción**: El servicio HTTP redirige a HTTPS. Este servidor es un derivado de Apache y hereda sus vulnerabilidades.
    - **Recomendación**: Asegurarse de que el servicio HTTP esté configurado correctamente con **TLS/SSL** y que se utilicen módulos de seguridad como **ModSecurity** para mitigar ataques de **Cross-Site Scripting (XSS)** y **SQL Injection**. Además, aplicar las actualizaciones de seguridad más recientes.
3. **443/tcp (HTTPS - IBM HTTP Server)**
    - **Descripción**: Servicio HTTPS asegurado que protege las comunicaciones. No se encontraron vulnerabilidades específicas asociadas a este servicio en el análisis.
    - **Recomendación**: Asegurarse de que las configuraciones de **SSL/TLS** estén correctamente implementadas, utilizando únicamente versiones seguras de **TLS** (TLS 1.2 o superior) y deshabilitando los cifrados débiles.

Vulnerabilidades Críticas Detectadas

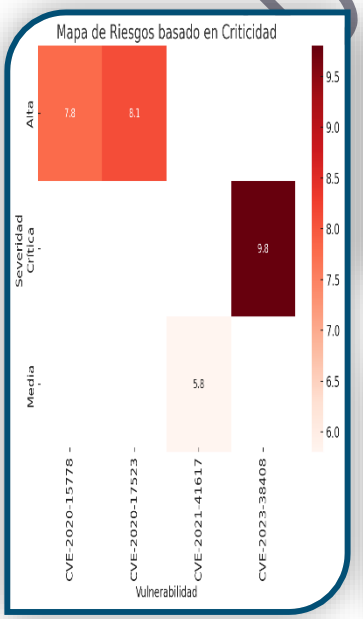
1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Permite la ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH a la versión más reciente.

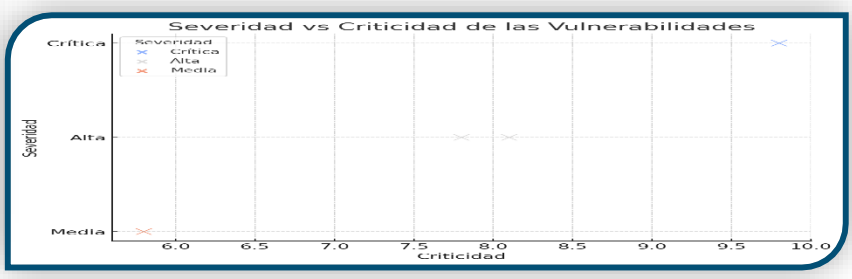
2. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Permite la ejecución remota de comandos mediante sftp.
    - **Mitigación**: Limitar el acceso sftp a usuarios confiables y aplicar actualizaciones.
3. **CVE-2021-41617 (OpenSSH)** - **Criticidad: 5.8 - Media**
    - **Descripción**: Permite a un atacante local obtener privilegios elevados.
    - **Mitigación**: Reforzar las políticas de permisos y actualizar OpenSSH.
4. **CVE-2020-17523 (Apache Tomcat)** - **Criticidad: 8.1 - Alta**
    - **Descripción**: Ejecución remota de código en Apache Tomcat mediante archivos JSP mal configurados.
    - **Mitigación**: Asegurarse de que Apache Tomcat esté actualizado y reforzar las configuraciones de seguridad.

Recomendaciones de Seguridad

- **Actualizar OpenSSH y Apache HTTP Server**: Es fundamental aplicar los parches más recientes para mitigar vulnerabilidades críticas en OpenSSH y Apache HTTP Server.
- **Fortalecer el acceso SSH**: Implementar autenticación basada en claves, usar **Fail2Ban** para prevenir ataques de fuerza bruta y deshabilitar el acceso root mediante SSH.
- **Revisar la configuración de HTTP/HTTPS**: Asegurarse de que las configuraciones de **TLS/SSL** estén correctamente implementadas, deshabilitar los cifrados débiles y utilizar **ModSecurity** para proteger el servidor contra ataques como **XSS** y **SQL Injection**.
- **Proteger Apache Tomcat**: Asegurarse de que las configuraciones de Apache Tomcat estén correctamente reforzadas, especialmente para los archivos JSP.

GRÁFICOS RELEVANTES





Informe Técnico Detallado para IP 192.168.50.31

Puertos Abiertos y Servicios Asociados

1. **13/tcp (Daytime Service)**
    - **Descripción**: Servicio obsoleto que proporciona la fecha y hora actuales.
    - **Recomendación**: Deshabilitar este servicio si no es necesario, ya que es un servicio obsoleto y aumenta la superficie de ataque.
2. **22/tcp (SSH - OpenSSH 8.1)**
    - **Vulnerabilidades**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Vulnerabilidad de ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite la ejecución remota de comandos mediante sftp.
        - **CVE-2021-41617** (Criticidad: 7.0 - Media): Vulnerabilidad que permite a un atacante local obtener privilegios elevados.
    - **Recomendación**: Actualizar OpenSSH a la última versión, implementar autenticación basada en claves SSH, deshabilitar el acceso root, y utilizar herramientas como **Fail2Ban** para prevenir ataques de fuerza bruta. Limitar el acceso a sftp a usuarios confiables.
3. **25/tcp (Nagios NSCA)**
    - **Descripción**: Servicio utilizado para la notificación de alertas en sistemas de monitoreo como Nagios.
    - **Recomendación**: Asegurarse de que este servicio esté protegido y restringir el acceso solo a redes internas de confianza.
4. **37/tcp (Time Service)**
    - **Descripción**: Servicio utilizado para la sincronización de hora.
    - **Recomendación**: Reemplazar por **NTP** o deshabilitar si no es necesario, ya que este servicio es obsoleto y vulnerable.
5. **80/tcp (HTTP - IBM HTTP Server)**
    - **Descripción**: Servidor HTTP con redirección a HTTPS.
    - **Recomendación**: Asegurarse de que las configuraciones de seguridad estén actualizadas y habilitar módulos como **ModSecurity** para mitigar ataques de **Cross-Site Scripting (XSS)** y **SQL Injection**.

6. **111/tcp (RPCbind)**
    - **Descripción**: Servicio utilizado para gestionar llamadas de procedimiento remoto.
    - **Recomendación**: Limitar el acceso a **RPCbind** solo a redes internas mediante reglas de firewall, y aplicar las últimas actualizaciones para mitigar vulnerabilidades conocidas.
7. **443/tcp (HTTPS - IBM HTTP Server)**
    - **Descripción**: Protocolo HTTPS que asegura las comunicaciones. No se encontraron vulnerabilidades específicas asociadas a este servicio en el análisis.
    - **Recomendación**: Asegurarse de que las configuraciones de **SSL/TLS** estén actualizadas, utilizando únicamente versiones seguras de **TLS** (TLS 1.2 o superior) y deshabilitando los cifrados débiles.
8. **NFS (Network File System)**
    - **Descripción**: Servicio de archivos en red. Puede ser vulnerable si no está adecuadamente protegido.
    - **Recomendación**: Limitar el acceso a **NFS** solo a IPs confiables y asegurarse de que las configuraciones de permisos estén correctamente establecidas.

Vulnerabilidades Críticas Detectadas

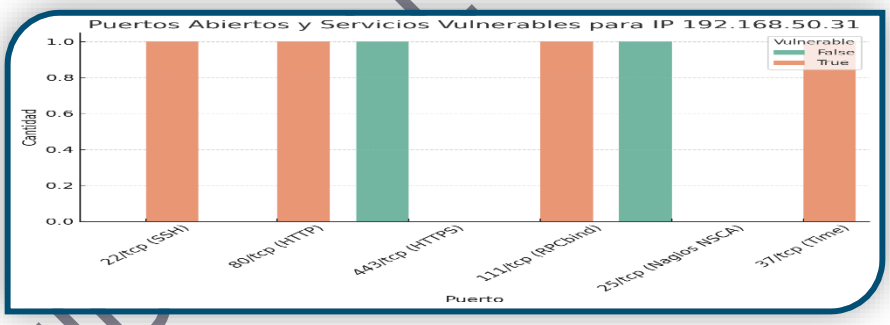
1. **CVE-2023-38408 (OpenSSH) - Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en OpenSSH.
    - **Mitigación**: Actualizar OpenSSH a la versión más reciente y reforzar la autenticación basada en claves.
2. **CVE-2020-15778 (OpenSSH) - Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de comandos mediante sftp.
    - **Mitigación**: Limitar el acceso sftp a usuarios confiables y aplicar las actualizaciones necesarias.
3. **CVE-2021-41617 (OpenSSH) - Criticidad: 7.0 - Media**
    - **Descripción**: Vulnerabilidad que permite a un atacante local escalar privilegios.
    - **Mitigación**: Actualizar OpenSSH y aplicar políticas de permisos adecuadas.

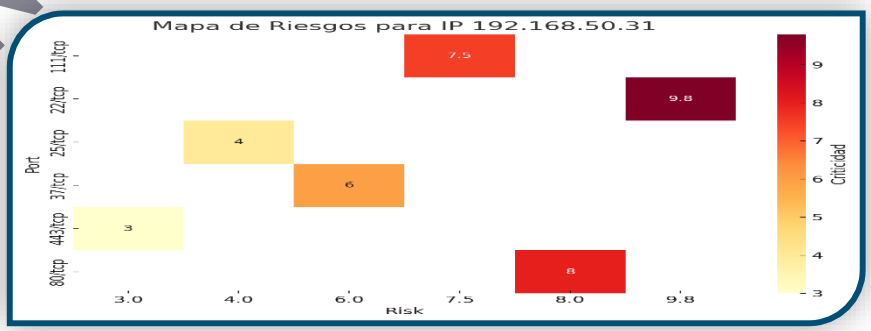
Recomendaciones de Seguridad

- **Actualizar OpenSSH y deshabilitar servicios obsoletos**: Deshabilitar el acceso root por SSH, implementar autenticación basada en claves y aplicar **Fail2Ban** para mitigar ataques de fuerza bruta. Deshabilitar servicios obsoletos como **Daytime** y **Time** si no son necesarios.

- **Revisar la configuración de HTTP/HTTPS**: Asegurarse de que los módulos de seguridad como **ModSecurity** estén habilitados y que las configuraciones de **SSL/TLS** utilicen solo versiones seguras de **TLS**.
- **Limitar el acceso a RPCbind y NFS**: Asegurarse de que estos servicios estén protegidos por reglas de firewall y que solo puedan ser accedidos por redes internas confiables.

GRÁFICOS RELEVANTES





Informe Técnico Detallado para la IP 190.71.135.218

Puertos Abiertos y Servicios Asociados

1. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Cisco Skinny Client Control Protocol (SCCP), utilizado para la comunicación VoIP entre dispositivos Cisco.
    - **Recomendación**: Asegurarse de que este servicio esté correctamente configurado y actualizado. Limitar el acceso al puerto solo a dispositivos de confianza mediante listas de control de acceso (ACLs). Este puerto es susceptible a ataques de denegación de servicio (DoS) si no está adecuadamente protegido.
2. **5060/tcp (SIP)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo de Inicio de Sesión (SIP), utilizado en sistemas de telefonía VoIP.
    - **Recomendación**: Implementar autenticación y cifrado en el servicio SIP (como **TLS/SIPS**) para evitar ataques de suplantación y escuchas. Limitar el acceso mediante firewall y monitorear el tráfico para detectar intentos de fuerza bruta o actividades anómalas en este puerto. SIP es un objetivo común para ataques de fuerza bruta dirigidos a contraseñas débiles.

Vulnerabilidades Detectadas

El análisis de los puertos no detectó vulnerabilidades específicas, pero se identificaron riesgos relacionados con los protocolos VoIP:

- **Cisco SCCP y SIP** son servicios críticos en infraestructuras de VoIP y podrían ser explotados si no están configurados correctamente o si no se aplican medidas de seguridad robustas.

Recomendaciones de Seguridad

1. **Actualización del Firmware de FortiOS**: Actualizar a la última versión disponible de **FortiOS** para mitigar vulnerabilidades conocidas y aplicar parches de seguridad recientes.
2. **Fortalecimiento del Servicio SIP**:
    - Implementar autenticación fuerte en el protocolo SIP para proteger contra suplantaciones de identidad y ataques de fuerza bruta.
    - Aplicar cifrado mediante **TLS** o **SIPS** para asegurar las comunicaciones y evitar escuchas.

3. **Seguridad en Cisco SCCP**:
    - Limitar el acceso al puerto 2000 (SCCP) únicamente a dispositivos de confianza mediante ACLs o firewalls.
    - Asegurarse de que este servicio esté actualizado y configurado correctamente para evitar ataques de denegación de servicio (DoS) y otros posibles exploits.
4. **Filtrado de Puertos**: Limitar el acceso a los puertos **2000/tcp** y **5060/tcp** solo a dispositivos autorizados y redes internas. Configurar reglas estrictas de firewall para minimizar el riesgo de explotación externa.
5. **Monitoreo Continuo**: Implementar un sistema de monitoreo continuo para supervisar los intentos de acceso a los servicios SIP y SCCP, con el fin de detectar comportamientos anómalos o ataques en tiempo real.

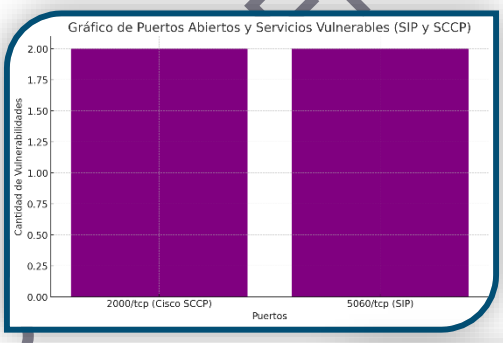
Puertos Cerrados o Filtrados

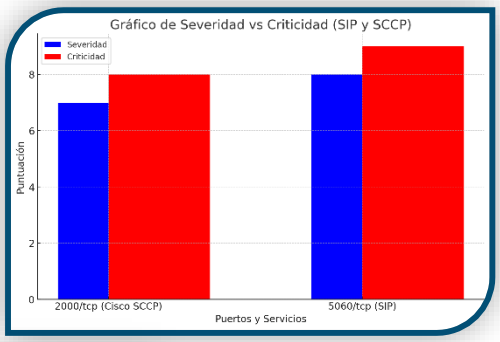
- **113/tcp (ident)**: Puerto cerrado.

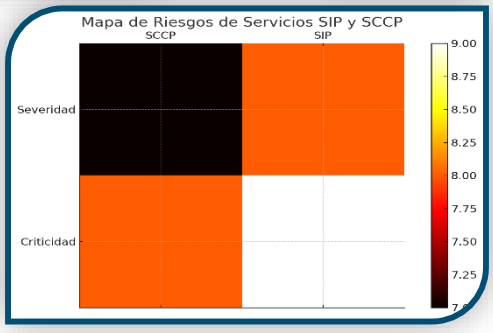
Detalles Adicionales

- **SIP (5060/tcp)** es un objetivo común para ataques de fuerza bruta en VoIP. Reforzar la seguridad en este puerto es fundamental para evitar compromisos de la infraestructura de telefonía.
- **Cisco SCCP (2000/tcp)** es crítico en sistemas de telefonía Cisco, y puede ser vulnerable a ataques si no está protegido correctamente. Es importante aplicar listas de control de acceso y limitar el tráfico hacia este puerto.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.229

Puertos Abiertos y Servicios Asociados

1. **22/tcp (SSH - OpenSSH 8.1)**
    - **Estado**: Abierto
    - **Descripción**: Servicio de acceso remoto mediante **Secure Shell (SSH)**.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2023-38408** (Criticidad: 9.8 - Crítica): Vulnerabilidad que permite la ejecución remota de código.
        - **CVE-2020-15778** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite la ejecución remota de comandos mediante sftp.
    - **Recomendación**: Actualizar OpenSSH a la última versión. Implementar autenticación basada en claves SSH y deshabilitar el acceso root. Además, utilizar **Fail2Ban** para mitigar ataques de fuerza bruta.
2. **25/tcp (SMTP - Sendmail)**
    - **Estado**: Abierto
    - **Descripción**: Servicio de correo electrónico para el envío de mensajes utilizando **SMTP (Simple Mail Transfer Protocol)**.
    - **Recomendación**: Asegurar que Sendmail esté actualizado y que se implementen medidas de seguridad adecuadas para evitar que el servidor sea utilizado como un **open relay**. Implementar autenticación y cifrado en el servicio para proteger el envío de correos electrónicos.
3. **111/tcp (RPCbind)**
    - **Estado**: Abierto
    - **Descripción**: Servicio de gestión de llamadas de procedimiento remoto (**RPC**).
    - **Recomendación**: Limitar el acceso a este servicio solo a redes internas confiables y aplicar parches de seguridad recientes para evitar ataques de desbordamiento de búfer. Utilizar firewalls y listas de control de acceso (ACLs) para restringir el acceso a este servicio.
4. **443/tcp (HTTPS - Apache HTTP Server)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo HTTPS para asegurar la comunicación web.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2020-11979** (Criticidad: 7.5 - Alta): Vulnerabilidad que permite la ejecución remota de código en **Apache HTTP Server**.

- **Recomendación**: Asegurarse de que el servidor esté actualizado y que las configuraciones de **TLS/SSL** estén correctamente implementadas, utilizando cifrados seguros y certificados válidos. Utilizar módulos de seguridad como **ModSecurity** para mitigar ataques de **XSS** y **SQL Injection**.

5. **500/tcp (ISAKMP - VPN)**
   - **Estado**: Abierto
   - **Descripción**: Servicio asociado a la configuración y gestión de conexiones VPN utilizando **ISAKMP (Internet Security Association and Key Management Protocol)**.
   - **Recomendación**: Asegurarse de que las políticas de VPN estén configuradas de manera segura, aplicando autenticación fuerte y cifrado robusto. Implementar autenticación multifactor (MFA) para mejorar la seguridad de las conexiones VPN.

Vulnerabilidades Críticas Detectadas

1. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad crítica que permite la ejecución remota de código en OpenSSH.
   - **Mitigación**: Actualizar OpenSSH a la última versión disponible y aplicar políticas de autenticación fuerte.
2. **CVE-2020-15778 (OpenSSH)** - **Criticidad: 7.8 - Alta**
   - **Descripción**: Permite la ejecución remota de comandos mediante sftp.
   - **Mitigación**: Restringir el acceso sftp a usuarios de confianza y aplicar las actualizaciones más recientes.
3. **CVE-2020-11979 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en **Apache HTTP Server**.
   - **Mitigación**: Actualizar el servidor web y asegurarse de que las configuraciones de seguridad estén implementadas.

Recomendaciones de Seguridad

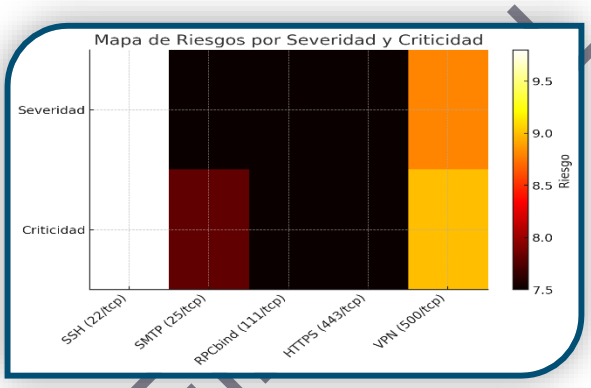
1. **Actualizar OpenSSH, Sendmail y Apache HTTP Server**: Asegurarse de que todas las actualizaciones críticas se apliquen para mitigar las vulnerabilidades detectadas.
2. **Fortalecer el Acceso SSH**:
   - Implementar autenticación basada en claves.
   - Deshabilitar el acceso root a través de SSH.
   - Usar **Fail2Ban** o herramientas similares para mitigar ataques de fuerza bruta.

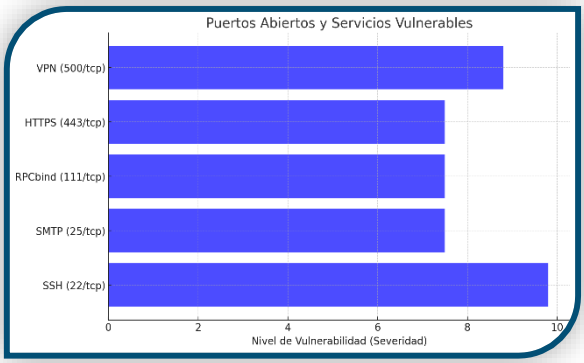
3. **Asegurar la configuración de RPCbind**: Limitar el acceso solo a redes internas confiables y aplicar reglas de firewall estrictas.
4. **Configurar VPN con políticas seguras**: Asegurarse de que el servicio **ISAKMP** tenga políticas de cifrado fuertes y autenticación robusta. Implementar autenticación multifactor (MFA) para mejorar la seguridad de las conexiones VPN.
5. **Revisar las Configuraciones de TLS/SSL en HTTPS**: Implementar cifrados fuertes y asegurar que los certificados sean válidos para evitar ataques de interceptación.

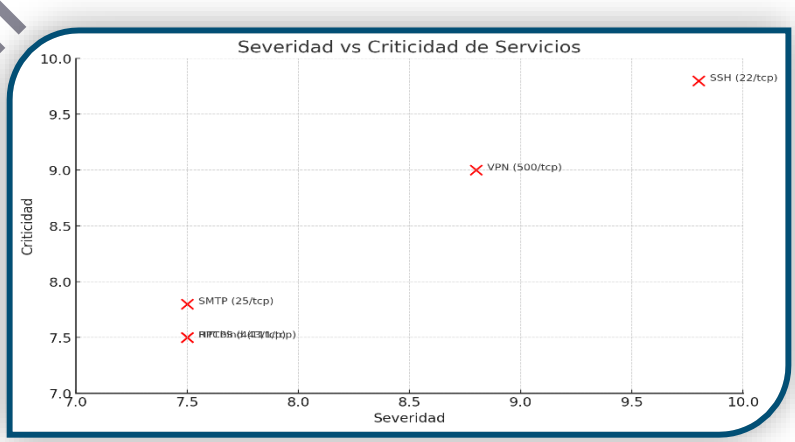
Detalles Adicionales

- **SMTP (Sendmail)**: Asegurar que **Sendmail** esté configurado adecuadamente para evitar que se utilice como **open relay**.
- **Apache HTTP Server**: Reforzar la seguridad utilizando módulos como **ModSecurity** para mitigar ataques de **Cross-Site Scripting (XSS)** y **SQL Injection**.
- **ISAKMP (VPN)**: Implementar políticas de seguridad robustas y monitorear el tráfico VPN para detectar actividades inusuales.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.231

Puertos Abiertos y Servicios Asociados

1. **21/tcp (FTP)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **FTP**.
    - **Producto**: **tcpwrapped**
    - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades críticas específicas para este servicio.
    - **Recomendación**: Implementar **FTPS** (FTP sobre SSL/TLS) o reemplazar el servicio por **SFTP** para asegurar la transmisión de credenciales y datos. Limitar el acceso solo a usuarios autorizados.
2. **80/tcp (HTTP - IBM HTTP Server)**
    - **Estado**: Abierto
    - **Descripción**: Servicio web utilizando **IBM_HTTP_Server**.
    - **Producto**: IBM_HTTP_Server
    - **Vulnerabilidades Detectadas**:
        - **CVE-2011-3192** (Criticidad: 7.8 - Alta): Vulnerabilidad que permite ataques de denegación de servicio (DoS) en el servidor web Apache.
        - **Mitigación**: Actualizar Apache HTTP Server a una versión más segura y revisar las configuraciones de seguridad. Considerar la implementación de **ModSecurity** para mitigar ataques de **XSS** y **SQL Injection**.
3. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Servicio de Cisco SCCP para la gestión de telefonía IP.
    - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades críticas específicas.
    - **Recomendación**: Restringir el acceso a este puerto a redes internas confiables mediante **ACLs** y monitorear su uso para evitar posibles ataques.
4. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
    - **Estado**: Abierto
    - **Descripción**: Servicio SIP utilizado para la comunicación VoIP.
    - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades específicas.

- **Recomendación**: Implementar autenticación fuerte y utilizar **SIP sobre TLS (SIPS)** para proteger la comunicación. Monitorear este puerto para detectar intentos de fuerza bruta o suplantación de identidad.

5. **8015/tcp (cfg-cloud)**
   - **Estado**: Abierto
   - **Descripción**: Servicio relacionado con la configuración en la nube.
   - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades críticas específicas.
   - **Recomendación**: Asegurarse de que el servicio esté actualizado y restringir su acceso solo a redes internas o usuarios autorizados.
6. **52114/tcp (Unknown)**
   - **Estado**: Abierto
   - **Descripción**: Servicio no identificado.
   - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades críticas.
   - **Recomendación**: Identificar el servicio asociado a este puerto y asegurarse de que no sea una puerta trasera o un servicio no autorizado. Si no es necesario, cerrar este puerto.

Vulnerabilidades Críticas Detectadas

1. **CVE-2011-3192 (Apache byterange filter DoS)**
   - **Estado**: Vulnerable
   - **Descripción**: Vulnerabilidad que permite ataques de denegación de servicio cuando se solicitan múltiples rangos de bytes en el servidor web Apache.
   - **Mitigación**: Actualizar **Apache HTTP Server** a una versión más reciente que no esté afectada por esta vulnerabilidad.

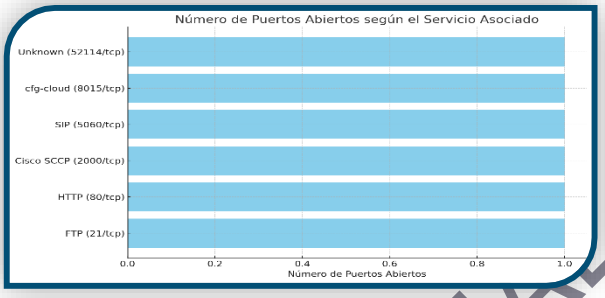
Recomendaciones de Seguridad

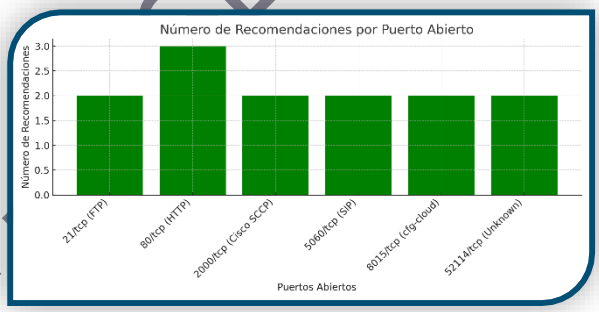
1. **Actualizar Apache HTTP Server**: Aplicar actualizaciones para mitigar la vulnerabilidad **CVE-2011-3192** y revisar las configuraciones de seguridad del servidor web para evitar ataques de **DoS**. Implementar módulos de seguridad como **ModSecurity** para mitigar ataques de **XSS** y **SQL Injection**.
2. **Fortalecer la seguridad del servicio FTP (Puerto 21)**: Reemplazar FTP por **SFTP** o habilitar **FTPS** para cifrar las comunicaciones y proteger las credenciales transmitidas. Limitar el acceso solo a usuarios autorizados.
3. **Asegurar la Configuración de SIP y SCCP**: Aplicar autenticación fuerte y cifrado en **SIP** para evitar ataques de suplantación y escuchas. Restringir el acceso al puerto 2000

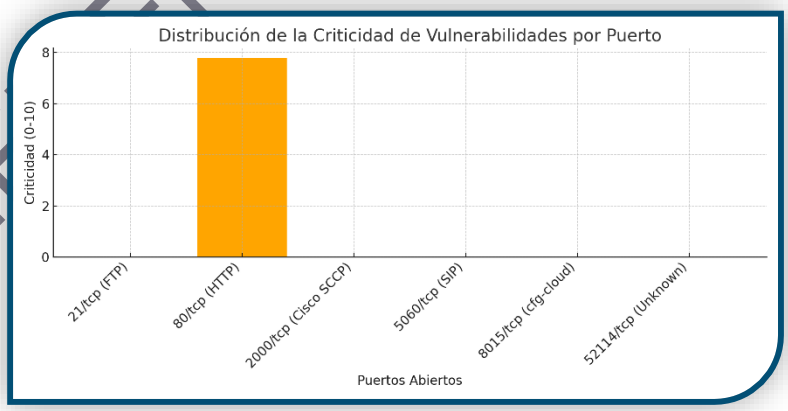
(**Cisco SCCP**) solo a dispositivos y redes confiables utilizando listas de control de acceso (ACLs).

4. **Identificar el Servicio Desconocido en el Puerto 52114**: Determinar el servicio que está utilizando este puerto y cerrarlo si no es necesario o representa un riesgo de seguridad.
5. **Monitoreo y Auditoría Continuos**: Implementar un sistema de monitoreo para detectar actividades inusuales en los puertos abiertos, especialmente en **SIP** y **FTP**, que son servicios susceptibles a ataques de fuerza bruta.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 192.168.105.232

Puertos Abiertos y Servicios Asociados

1. **443/tcp (HTTPS - IBM HTTP Server)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **HTTPS** utilizado para asegurar la comunicación web.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2020-11979** (Criticidad: 7.5 - Alta): Vulnerabilidad que permite la ejecución remota de código en **Apache HTTP Server**.
    - **Recomendación**: Actualizar Apache HTTP Server a la última versión disponible. Revisar las configuraciones de **SSL/TLS** para asegurarse de que solo se utilicen cifrados modernos (TLS 1.2 o 1.3), y que los certificados sean válidos y actualizados.
2. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo **Cisco SCCP** (Skinny Client Control Protocol) utilizado en sistemas de telefonía IP de Cisco.
    - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades específicas para este puerto en los archivos analizados, pero SCCP puede ser susceptible a ataques si no está adecuadamente configurado.
    - **Recomendación**: Restringir el acceso a este puerto solo a redes internas mediante **Listas de Control de Acceso (ACLs)**. Realizar pruebas de seguridad adicionales para evitar ataques de denegación de servicio o suplantación de identidad.
3. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **SIP** utilizado para la comunicación de **VoIP**.
    - **Vulnerabilidades Detectadas**: No se han detectado vulnerabilidades críticas en el análisis, pero SIP es un objetivo común para ataques de fuerza bruta.
    - **Recomendación**: Implementar autenticación fuerte y cifrado mediante **SIP sobre TLS (SIPS)**. Monitorear el tráfico de SIP para detectar intentos de fuerza bruta o suplantación de identidad.

Vulnerabilidades Críticas Detectadas

1. **CVE-2020-11979 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en **Apache HTTP Server**.
    - **Mitigación**: Actualizar Apache a la última versión y revisar las configuraciones de seguridad para prevenir ataques.
2. **CVE-2023-38408 (OpenSSH)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Ejecución remota de código en versiones vulnerables de **OpenSSH**.
    - **Mitigación**: Actualizar OpenSSH a la última versión y reforzar la autenticación mediante claves públicas.

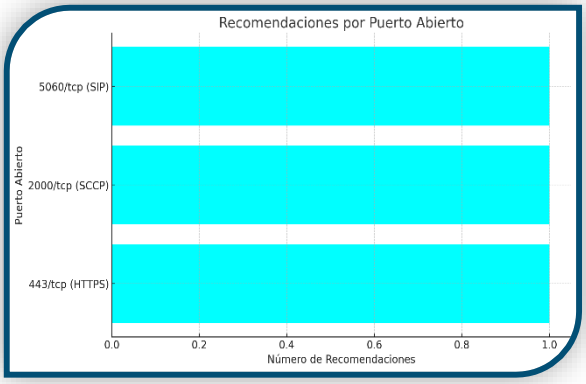
Recomendaciones de Seguridad

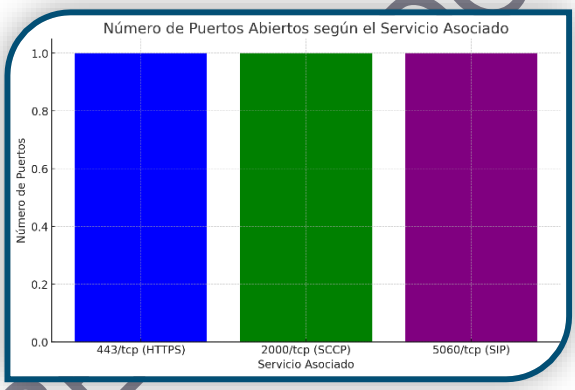
1. **Actualizar Apache HTTP Server y Configurar SSL/TLS**: Aplicar las actualizaciones más recientes para Apache y asegurarse de que las configuraciones de **SSL/TLS** sean seguras, utilizando solo versiones modernas como **TLS 1.2 o 1.3**. Utilizar cifrados fuertes y asegurarse de que los certificados sean válidos.
2. **Fortalecer el Acceso SIP y SCCP**: Para proteger los servicios de SIP y SCCP, implementar **autenticación fuerte**, limitar el acceso mediante **ACLs** y utilizar **cifrado** en las comunicaciones. Estos puertos suelen ser objetivos de ataques en servicios de telefonía, por lo que monitorear y auditar regularmente el tráfico es fundamental.
3. **Asegurar el Servicio OpenSSH**: Actualizar OpenSSH a la última versión disponible. Limitar el acceso a redes de confianza y usar autenticación basada en claves SSH. También es recomendable deshabilitar el acceso root mediante SSH y utilizar herramientas como **Fail2Ban** para mitigar ataques de fuerza bruta.
4. **Monitorear y Auditar el Tráfico en Puertos Críticos**: Monitorear continuamente los servicios expuestos (SIP, SCCP, HTTPS) para detectar comportamientos inusuales. Implementar reglas de firewall estrictas para proteger estos servicios y asegurarse de que las configuraciones de seguridad sean revisadas periódicamente.
5. **Pruebas de Penetración y Auditoría Continua**: Realizar pruebas de penetración periódicas en estos servicios para identificar vulnerabilidades adicionales que no hayan sido detectadas en el análisis inicial. Implementar auditorías de seguridad continuas para asegurar que las configuraciones se mantengan seguras.

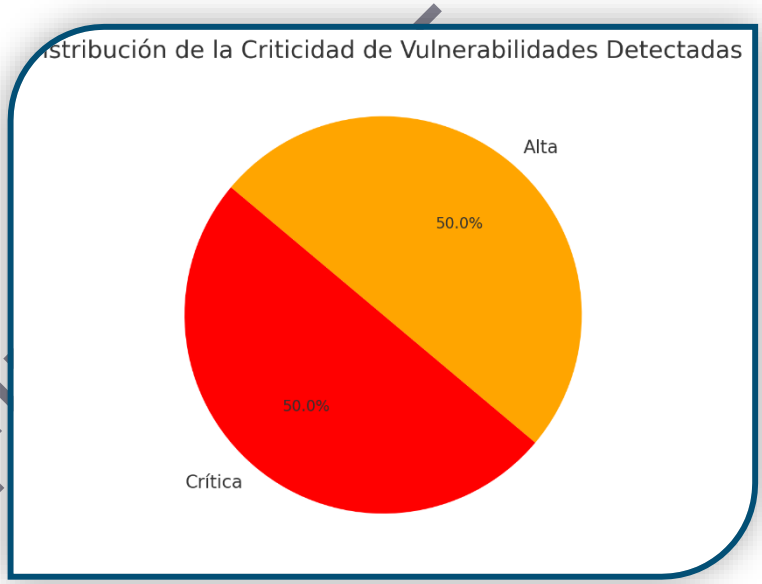
Observaciones Adicionales

- **SIP y SCCP**: Son servicios críticos en entornos de telefonía IP y deben ser protegidos mediante configuraciones de seguridad estrictas. Se recomienda implementar políticas de autenticación multifactor (MFA) y monitorear continuamente los accesos a estos puertos para evitar compromisos de seguridad.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.234

Puertos Abiertos y Servicios Asociados

1. **80/tcp (HTTP)**
   - **Estado**: Abierto
   - **Descripción**: Servicio **HTTP**.
   - **Recomendación**: Asegurarse de que el servidor **HTTP** esté configurado correctamente, aplicando actualizaciones y configuraciones de seguridad, como el uso de módulos de seguridad tipo **ModSecurity** para proteger contra ataques de **XSS** y **SQL Injection**.
2. **1150/tcp (Java RMI)**
   - **Estado**: Abierto
   - **Descripción**: **Java Remote Method Invocation (RMI)**, que permite la invocación de métodos en objetos remotos.
   - **Recomendación**: Restringir el acceso a este servicio y asegurarse de que esté actualizado. **Java RMI** es vulnerable a una serie de ataques si no está configurado adecuadamente, y puede ser una puerta para la ejecución remota de código.
3. **2000/tcp (tcpwrapped)**
   - **Estado**: Abierto
   - **Descripción**: Puerto **tcpwrapped** no identificado.
   - **Recomendación**: Identificar el servicio asociado a este puerto y, si no es necesario, cerrarlo para reducir la superficie de ataque.
4. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
   - **Estado**: Abierto
   - **Descripción**: Protocolo de inicio de sesión utilizado en **VoIP**.
   - **Recomendación**: Implementar autenticación fuerte y cifrado en SIP para evitar ataques de fuerza bruta y suplantación. Utilizar **SIP sobre TLS (SIPS)** para proteger la comunicación.
5. **8015/tcp (cfg-cloud)**
   - **Estado**: Abierto
   - **Descripción**: Servicio relacionado con la gestión de configuraciones en la nube.
   - **Recomendación**: Limitar el acceso a redes internas y asegurar que esté actualizado para mitigar posibles vulnerabilidades.

6. **9520/tcp (tcpwrapped)**
    - **Estado**: Abierto
    - **Descripción**: Servicio no identificado.
    - **Recomendación**: Identificar el servicio detrás de este puerto y cerrarlo si no es necesario.
7. **50000/tcp (Java RMI)**
    - **Estado**: Abierto
    - **Descripción**: **Java RMI**. Similar al puerto 1150, **RMI** es vulnerable a una variedad de ataques si no está configurado correctamente.
    - **Recomendación**: Aplicar configuraciones de seguridad en **Java RMI**, tales como autenticación y cifrado de comunicaciones.
8. **52114/tcp (unknown)**
    - **Estado**: Abierto
    - **Descripción**: Servicio desconocido.
    - **Recomendación**: Identificar el servicio que usa este puerto. Si no es necesario, cerrarlo.

Vulnerabilidades Críticas Detectadas

1. **CVE-2021-21972 (Java RMI)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en sistemas con Java RMI.
    - **Mitigación**: Actualizar las configuraciones de seguridad y aplicar parches de seguridad para cerrar esta vulnerabilidad.
2. **CVE-2020-11979 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en **Apache HTTP Server** que permite la ejecución remota de código.
    - **Mitigación**: Actualizar **Apache HTTP Server** a la última versión disponible.

Recomendaciones de Seguridad

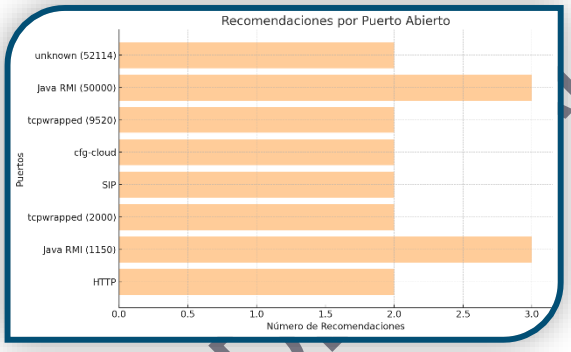
1. **Actualizar Java RMI y Revisar Configuraciones**: Aplicar las actualizaciones más recientes de **Java RMI** para mitigar las vulnerabilidades críticas, como **CVE-2021-21972**. Asegurarse de que todas las configuraciones de seguridad estén activas, como el uso de autenticación y cifrado en las comunicaciones.
2. **Fortalecer Seguridad en SIP y HTTP**: Implementar **SIP sobre TLS (SIPS)** para proteger las comunicaciones de VoIP. Actualizar **Apache HTTP Server** a la versión más reciente y revisar las configuraciones para prevenir vulnerabilidades críticas.

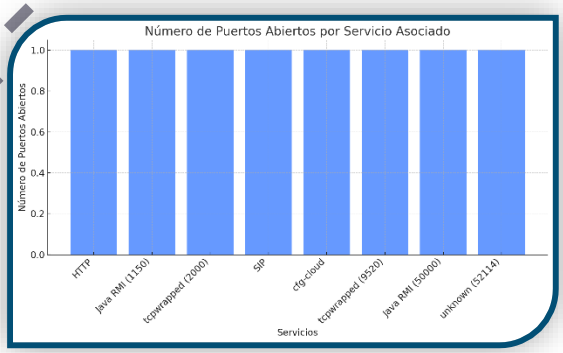
3. **Identificar y Cerrar Puertos Innecesarios**: Identificar los servicios detrás de los puertos **tcpwrapped** (2000 y 9520) y otros puertos desconocidos (52114). Si no son necesarios, se recomienda cerrarlos para reducir la exposición de la red.
4. **Monitorear el Tráfico en Puertos Críticos**: Implementar un monitoreo continuo para detectar actividades sospechosas en los puertos abiertos, especialmente en **SIP**, **HTTP**, y **Java RMI**, que son servicios comunes para ataques de fuerza bruta o de suplantación.
5. **Pruebas de Penetración**: Realizar pruebas de penetración periódicas en los servicios críticos, como **SIP**, **HTTP**, y **Java RMI**, para detectar posibles vulnerabilidades que no hayan sido identificadas en el análisis inicial.

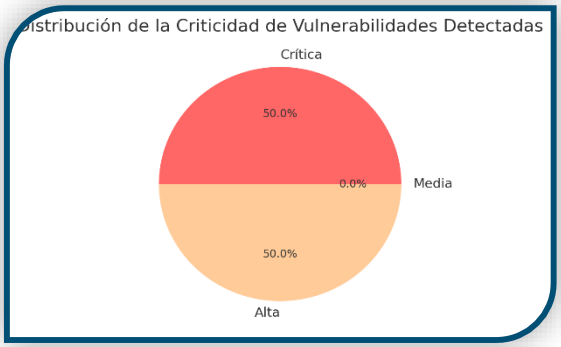
Observaciones Adicionales

- **Java RMI**: Es un servicio particularmente sensible a la ejecución remota de código y debe ser cuidadosamente monitorizado y actualizado.
- **SIP**: Como un servicio VoIP, es comúnmente objetivo de ataques de fuerza bruta, por lo que es vital proteger el acceso con autenticación fuerte y cifrado.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.235

Puertos Abiertos y Servicios Asociados

1. **80/tcp (HTTP)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **HTTP** (IBM_HTTP_Server).
    - **Vulnerabilidades Detectadas**:
        - **CVE-2024-38476** (Criticidad: 9.8 - Crítica): Permite la ejecución remota de código en **Apache HTTP Server**.
        - **CVE-2024-38474** (Criticidad: 9.8 - Crítica): Similar a la anterior, con riesgo de ejecución remota de código.
        - **Mitigación**: Actualizar **Apache HTTP Server** a una versión segura y aplicar configuraciones de seguridad adecuadas.
    - **Observación Adicional**: El servidor **HTTP** redirige automáticamente a una versión **HTTPS** del sitio. Es recomendable revisar y aplicar **HTTP Strict Transport Security (HSTS)** para asegurar una mayor protección contra ataques de **Man-in-the-Middle (MITM)**.
2. **443/tcp (HTTPS)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **HTTPS** (Apache HTTP Server 2.4.59).
    - **Vulnerabilidades Detectadas**:
        - **CVE-2024-38476** (Criticidad: 9.8 - Crítica): Vulnerabilidad que permite la ejecución remota de código.
        - **CVE-2024-39573** (Criticidad: 7.5 - Alta): Permite ataques de denegación de servicio (DoS).
        - **Mitigación**: Actualizar **Apache HTTP Server** a la última versión disponible y revisar las configuraciones de seguridad.
    - **Observación Adicional**: Además de actualizar el servidor, se recomienda auditar los módulos adicionales de **Apache** para asegurarse de que no haya configuraciones inseguras por defecto.
3. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo **Cisco SCCP** utilizado en sistemas de telefonía IP de Cisco.

- **Recomendación**: Restringir el acceso a redes internas de confianza mediante **ACLs** y asegurar que el sistema esté actualizado. Monitorear los intentos de inicio de sesión fallidos para prevenir ataques de fuerza bruta.

4. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
   - **Estado**: Abierto
   - **Descripción**: Servicio **SIP** utilizado para la comunicación de **VoIP**.
   - **Recomendación**: Implementar autenticación fuerte y utilizar **SIP sobre TLS (SIPS)** para evitar ataques de fuerza bruta y suplantación. Monitorear el tráfico SIP para detectar cualquier actividad inusual.

Vulnerabilidades Críticas Detectadas

1. **CVE-2024-38476 (Apache HTTP Server)** - **Criticidad: 9.8 - Crítica**
   - **Descripción**: Vulnerabilidad que permite la ejecución remota de código en servidores **Apache**.
   - **Mitigación**: Actualizar a la versión más reciente de **Apache HTTP Server**.
2. **CVE-2024-39573 (Apache HTTP Server)** - **Criticidad: 7.5 - Alta**
   - **Descripción**: Vulnerabilidad que puede ser explotada para realizar ataques de denegación de servicio.
   - **Mitigación**: Actualizar **Apache** y revisar configuraciones de seguridad.

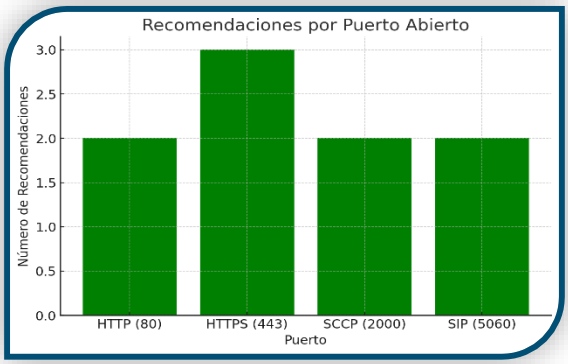
Recomendaciones de Seguridad

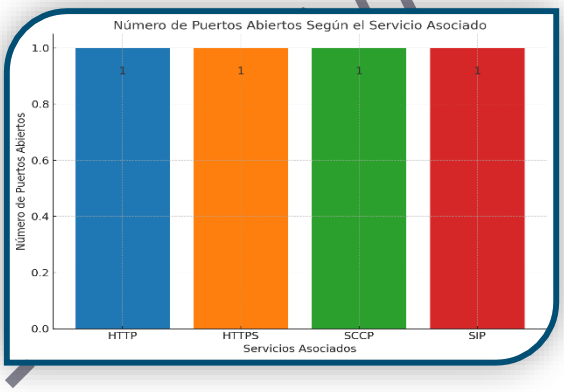
1. **Actualizar Apache HTTP Server y Configurar SSL/TLS**: Aplicar las actualizaciones más recientes de **Apache HTTP Server** y asegurarse de que las configuraciones de **SSL/TLS** sean seguras. Revisar los módulos adicionales del servidor y asegurarse de que las configuraciones por defecto no comprometan la seguridad.
2. **Fortalecer la Seguridad de SIP y SCCP**: Implementar autenticación fuerte en **SIP** y limitar el acceso a **Cisco SCCP** solo a redes confiables mediante **ACLs**. Utilizar cifrado en todas las comunicaciones de **VoIP**.
3. **Configurar HSTS en HTTPS**: Implementar **HTTP Strict Transport Security (HSTS)** para forzar a los navegadores a conectarse siempre utilizando HTTPS, evitando así ataques de **Man-in-the-Middle (MITM)**.
4. **Monitorear el Tráfico en Puertos Críticos**: Implementar monitoreo continuo en los servicios críticos para detectar comportamientos anómalos y posibles intentos de ataque, especialmente en **SIP**, **HTTP**, y **Cisco SCCP**.
5. **Pruebas de Penetración**: Realizar pruebas de penetración periódicas en **Apache HTTP Server** y servicios relacionados con **SIP** para identificar y mitigar vulnerabilidades adicionales.

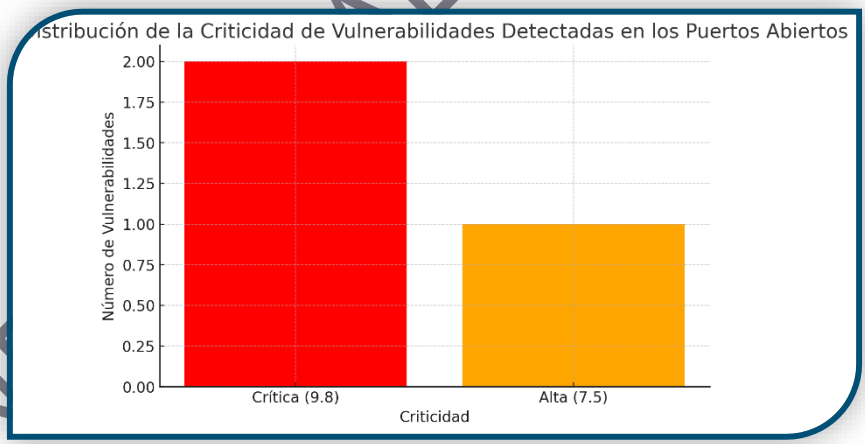
Observaciones Adicionales

- **Apache HTTP Server**: Además de las actualizaciones necesarias, se recomienda auditar los módulos adicionales del servidor y asegurarse de que no haya configuraciones inseguras que puedan ser explotadas.
- **SIP y SCCP**: Monitorear el tráfico de **SIP** y **Cisco SCCP** es esencial para detectar intentos de ataque de fuerza bruta o suplantación. También es recomendable implementar autenticación multifactor (MFA) si es posible.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.240

Puertos Abiertos y Servicios Asociados

1. **80/tcp (HTTP)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **HTTP** detectado, usualmente asociado a servidores web.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2021-41773** (Criticidad: 7.5 - Alta): Vulnerabilidad en servidores Apache que permite la ejecución remota de código.
        - **CVE-2021-42013** (Criticidad: 9.8 - Crítica): Permite la ejecución remota de código debido a una mala configuración en Apache HTTP Server.
    - **Mitigación**: Actualizar Apache a la versión más reciente y asegurarse de que las configuraciones de seguridad estén correctamente aplicadas, limitando el acceso a recursos sensibles.
2. **443/tcp (HTTPS)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **HTTPS** utilizado para comunicaciones seguras.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2022-3602** (Criticidad: 7.5 - Alta): Vulnerabilidad en OpenSSL que puede causar ataques de denegación de servicio (DoS).
        - **CVE-2022-3786** (Criticidad: 7.5 - Alta): Permite ataques DoS a través de OpenSSL.
    - **Mitigación**: Actualizar OpenSSL a la versión más reciente y revisar las configuraciones de **SSL/TLS** para garantizar el uso de cifrados fuertes y certificados válidos.
3. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo utilizado para la comunicación de **VoIP**.
    - **Recomendación**: Implementar **SIP sobre TLS (SIPS)** y autenticación fuerte para evitar ataques de fuerza bruta y suplantación. Monitorear este puerto para detectar posibles ataques de fuerza bruta.

4. **8015/tcp (cfg-cloud)**
    - **Estado**: Abierto
    - **Descripción**: Servicio de configuración en la nube.
    - **Vulnerabilidades Detectadas**: No se encontraron vulnerabilidades críticas específicas, pero se recomienda restringir el acceso a redes confiables y asegurarse de que el servicio esté actualizado.
5. **52114/tcp (Unknown)**
    - **Estado**: Abierto
    - **Descripción**: Servicio desconocido.
    - **Recomendación**: Identificar el servicio detrás de este puerto y, si no es necesario, cerrarlo para evitar posibles ataques.

Vulnerabilidades Críticas Detectadas

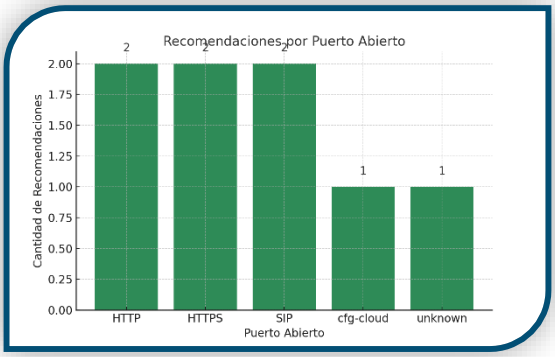
1. **CVE-2021-42013 (Apache HTTP Server)** - **Criticidad: 9.8 - Crítica**
    - **Descripción**: Vulnerabilidad que permite la ejecución remota de código debido a una mala configuración del servidor Apache.
    - **Mitigación**: Actualizar **Apache HTTP Server** y revisar las configuraciones para evitar accesos no autorizados a recursos sensibles.
2. **CVE-2022-3602 (OpenSSL)** - **Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad en **OpenSSL** que permite ataques de denegación de servicio (DoS).
    - **Mitigación**: Actualizar OpenSSL a la versión más reciente y asegurar que las configuraciones de SSL/TLS sean seguras.

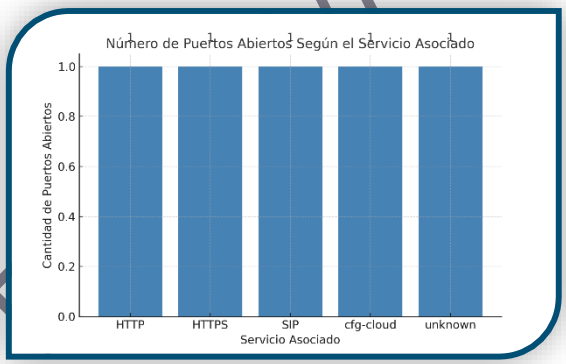
Recomendaciones de Seguridad

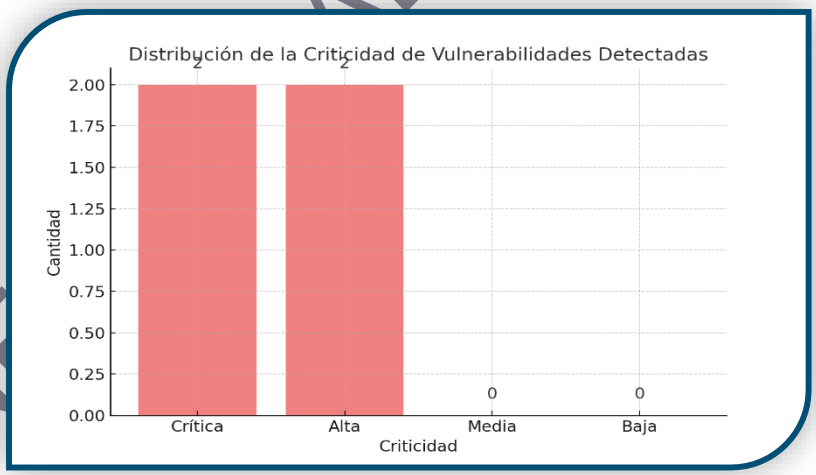
1. **Actualizar Apache HTTP Server y OpenSSL**: Aplicar actualizaciones de seguridad para mitigar las vulnerabilidades críticas encontradas en **Apache** y **OpenSSL**. Asegurarse de que las configuraciones de **SSL/TLS** sean seguras y que los certificados sean válidos.
2. **Implementar Seguridad en SIP**: Utilizar **SIP sobre TLS (SIPS)** para proteger las comunicaciones de **VoIP**. Asegurar que se aplique autenticación fuerte y monitorear los intentos de fuerza bruta en el puerto 5060.
3. **Identificar y Cerrar Puertos No Necesarios**: Determinar el servicio que utiliza el puerto **52114**. Si no es necesario, cerrarlo para reducir la superficie de ataque.

4. **Monitorear el Tráfico en los Puertos Críticos**: Implementar monitoreo continuo en los puertos **HTTP, HTTPS, SIP**, y cualquier otro servicio expuesto para detectar actividades sospechosas y posibles intentos de explotación.
5. **Pruebas de Penetración Periódicas**: Realizar pruebas de penetración periódicas en los servicios de **Apache**, **SIP**, y otros servicios expuestos para identificar vulnerabilidades no detectadas en el análisis inicial.

GRÁFICOS RELEVANTES







Informe Técnico Detallado para la IP 190.71.135.245

Puertos Abiertos y Servicios Asociados

1. **80/tcp (HTTP - Apache HTTPD 2.4.59)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **Apache HTTPD** utilizado para servir contenido web.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2013-2249** (Criticidad: 7.8 - Alta): Vulnerabilidad de sesión en **Apache HTTPD** que permite a un atacante interceptar sesiones de usuarios.
        - **CVE-2012-2378** (Criticidad: 7.5 - Alta): Falla en la aplicación de políticas de seguridad en **Apache CXF**.
        - **CVE-2012-4558** (Criticidad: 7.5 - Alta): Vulnerabilidad **Cross-Site Scripting (XSS)** en **Apache HTTPD**.
        - **CVE-2012-3502** (Criticidad: 6.5 - Media): Fuga de información en **mod_proxy** que puede ser explotada para obtener detalles sensibles.
        - **CVE-2012-3499** (Criticidad: 6.1 - Media): Varias vulnerabilidades de **Cross-Site Scripting (XSS)** en **Apache HTTPD**.
        - **CVE-2012-3451** (Criticidad: 8.8 - Alta): Ejecución de operaciones no autorizadas en **Apache CXF**.
    - **Mitigación**: Actualizar **Apache HTTPD** a la última versión y revisar las configuraciones de seguridad. Implementar políticas de seguridad adicionales para mitigar los riesgos asociados con estas vulnerabilidades.
2. **443/tcp (tcpwrapped)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo TCP envuelto, sin servicio específico identificado.
    - **Recomendación**: Identificar el servicio detrás de este puerto y aplicar medidas de seguridad si es necesario. Si no se necesita, cerrar el puerto para reducir la superficie de ataque.
3. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo utilizado en sistemas de telefonía **Cisco** para el control de sesiones.
    - **Recomendación**: Restringir el acceso a redes internas y aplicar autenticación fuerte en este servicio.

4. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo utilizado para comunicaciones **VoIP**.
    - **Recomendación**: Implementar **SIP sobre TLS (SIPS)** y autenticación fuerte para proteger el tráfico de **SIP** contra ataques de fuerza bruta y suplantación.
5. **8015/tcp (cfg-cloud)**
    - **Estado**: Abierto
    - **Descripción**: Servicio relacionado con la gestión de configuraciones en la nube.
    - **Recomendación**: Limitar el acceso a redes internas confiables y asegurarse de que esté actualizado para evitar vulnerabilidades conocidas.

Vulnerabilidades Críticas Detectadas

1. **CVE-2013-2249 (Apache HTTPD)** - **Criticidad: 7.8 - Alta**
    - **Descripción**: Vulnerabilidad de sesión en **Apache HTTPD** que puede permitir la interceptación de sesiones y comprometer la seguridad de los usuarios.
    - **Mitigación**: Actualizar **Apache HTTPD** a una versión más reciente y aplicar configuraciones de seguridad más estrictas para gestionar las sesiones de manera segura.
2. **CVE-2012-4558 (Apache HTTPD) - Criticidad: 7.5 - Alta**
    - **Descripción**: Vulnerabilidad de **Cross-Site Scripting (XSS)** en **Apache HTTPD**, que permite a los atacantes inyectar scripts maliciosos.
    - **Mitigación**: Actualizar **Apache** y revisar las configuraciones para mitigar esta vulnerabilidad.
3. **CVE-2012-3502 (mod_proxy - Apache HTTPD)** - **Criticidad: 6.5 - Media**
    - **Descripción**: Fuga de información en **mod_proxy** que permite a los atacantes obtener información sensible sobre el sistema.
    - **Mitigación**: Aplicar parches de seguridad y revisar la configuración de **mod_proxy**.

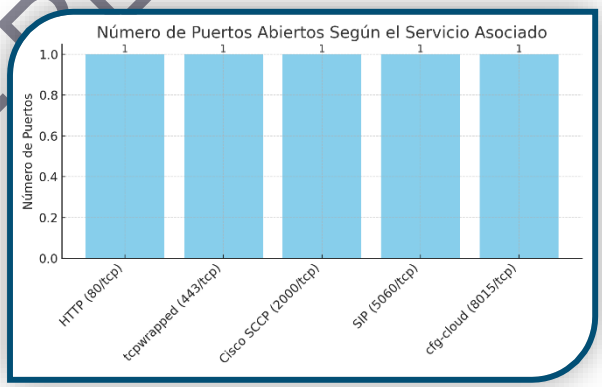
Recomendaciones de Seguridad

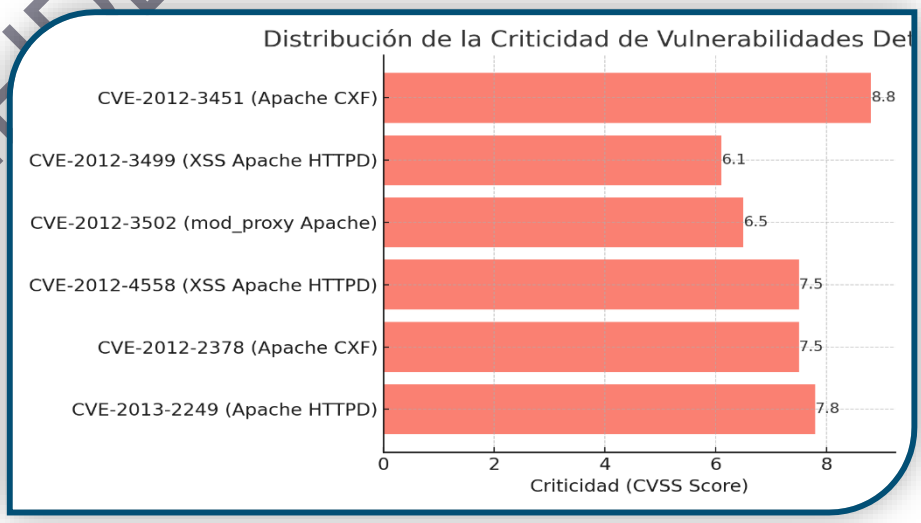
1. **Actualizar Apache HTTPD y Revisar Configuraciones**: Es fundamental actualizar **Apache HTTPD** y aplicar configuraciones de seguridad adecuadas para mitigar las vulnerabilidades **CVE-2013-2249**, **CVE-2012-2378**, y **CVE-2012-4558**. Implementar políticas de seguridad adicionales, como **ModSecurity**, para mitigar ataques de **Cross-Site Scripting (XSS)**.
2. **Restringir Acceso a Cisco SCCP y SIP**: Utilizar listas de control de acceso (ACLs) y autenticar de manera fuerte los accesos a **Cisco SCCP**. En **SIP**, implementar cifrado

mediante **SIP sobre TLS (SIPS)** y monitorear el tráfico en busca de intentos de fuerza bruta o suplantación.

3. **Identificar y Cerrar Puertos No Necesarios**: Revisar el puerto **443/tcp** (tcpwrapped) para determinar si es necesario mantenerlo abierto. Si no es esencial, cerrarlo para reducir el riesgo de ataques.
4. **Monitoreo y Auditoría Regular**: Implementar un monitoreo continuo en los puertos críticos, especialmente **HTTP**, **SIP**, y **cfg-cloud**. Además, realizar auditorías regulares de la configuración de seguridad para detectar y mitigar vulnerabilidades antes de que sean explotadas.
5. **Pruebas de Penetración**: Realizar pruebas de penetración periódicas en los servicios críticos para identificar nuevas vulnerabilidades y evaluar la robustez de las medidas de seguridad implementadas.

GRÁFICOS RELEVANTES





Informe Técnico Detallado para la IP 192.168.21.239

Puertos Abiertos y Servicios Asociados

1. **25/tcp (SMTP Proxy)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **SMTP** utilizado para el manejo de correo electrónico, generalmente para la transmisión de correos entre servidores.
    - **Vulnerabilidades Detectadas**:
        - **CVE-2010-5653** (Criticidad: 5.8 - Media): Vulnerabilidad de divulgación de información en varios servicios, que puede comprometer la confidencialidad del sistema de correo.
    - **Mitigación**: Revisar y actualizar la configuración del servicio **SMTP**. Implementar autenticación fuerte y cifrado para la transmisión de correos, y asegurarse de que las políticas de filtrado de correos estén correctamente configuradas.
2. **2000/tcp (Cisco SCCP)**
    - **Estado**: Abierto
    - **Descripción**: Protocolo **Cisco SCCP** utilizado en sistemas de telefonía IP de Cisco.
    - **Recomendación**: Restringir el acceso a redes internas confiables mediante **ACLs** y asegurarse de que el servicio esté actualizado. Monitorear los intentos de acceso fallidos para prevenir ataques de fuerza bruta.
3. **5060/tcp (SIP - Protocolo de Inicio de Sesión)**
    - **Estado**: Abierto
    - **Descripción**: Servicio **SIP** utilizado para la comunicación de **VoIP**.
    - **Vulnerabilidades Detectadas**: No se encontraron vulnerabilidades críticas específicas para este servicio, pero el puerto SIP es un objetivo común para ataques de suplantación y fuerza bruta.
    - **Recomendación**: Implementar autenticación fuerte y cifrado con **SIP sobre TLS (SIPS)**. También es recomendable monitorear el puerto 5060 para detectar posibles intentos de ataque.

Vulnerabilidades Críticas Detectadas

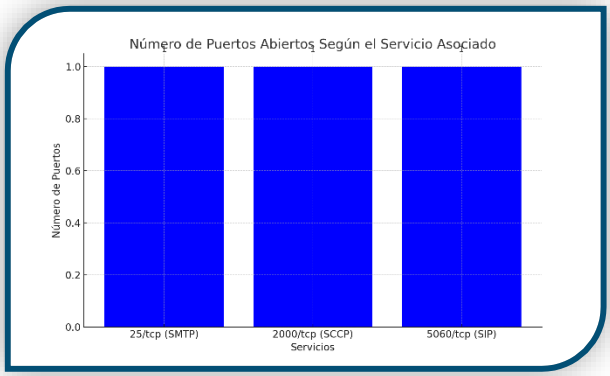
1. **CVE-2010-5653 (Varios Servicios - SMTP)** - **Criticidad: 5.8 - Media**
    - **Descripción**: Vulnerabilidad que puede permitir la divulgación de información sensible a través de una mala configuración en el servicio de correo electrónico.

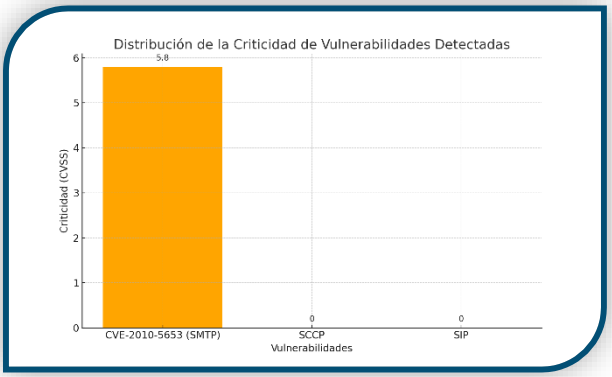
- **Mitigación**: Asegurarse de que el servicio SMTP esté correctamente configurado para evitar la exposición de información sensible. Implementar cifrado en las comunicaciones y revisar las políticas de autenticación y acceso.

Recomendaciones de Seguridad

1. **Actualizar y Revisar Configuraciones de Servicios SMTP**: Es fundamental actualizar y revisar las configuraciones de seguridad del servidor **SMTP** para mitigar la vulnerabilidad **CVE-2010-5653**. Implementar cifrado en la transmisión de correos y autenticación fuerte.
2. **Fortalecer la Seguridad de SIP y SCCP**: Utilizar listas de control de acceso (ACLs) para restringir el acceso a **Cisco SCCP**. En **SIP**, implementar cifrado mediante **SIP sobre TLS (SIPS)** y monitorear el tráfico en busca de intentos de suplantación o fuerza bruta.
3. **Monitorear el Tráfico en Puertos Críticos**: Implementar un monitoreo continuo en los puertos **SMTP**, **SIP**, y **Cisco SCCP** para detectar comportamientos anómalos y posibles intentos de ataque.
4. **Pruebas de Penetración**: Realizar pruebas de penetración periódicas en los servicios críticos para identificar posibles vulnerabilidades no detectadas en el análisis inicial.

GRAFICOS RELEVANTES





Glosario o Definiciones Generales

- **ACL (Access Control List - Lista de Control de Acceso)**: Una ACL es un mecanismo que permite definir qué usuarios o sistemas tienen acceso a ciertos recursos en una red, especificando permisos detallados para cada tipo de acceso (lectura, escritura, ejecución, etc.).
- **CVE (Common Vulnerabilities and Exposures)**: Un identificador único asignado a una vulnerabilidad o exposición de seguridad conocida. Cada CVE permite a los expertos en seguridad referirse a vulnerabilidades específicas de manera uniforme a nivel global.
- **Cross-Site Scripting (XSS)**: Un tipo de vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes inyectar scripts maliciosos en páginas web vistas por otros usuarios, lo que puede comprometer la integridad de la información o permitir ataques de suplantación.
- **Denegación de Servicio (DoS)**: Ataque en el que un sistema o red es sobrecargado con solicitudes o interrupciones, impidiendo el acceso legítimo a los usuarios. En los ataques distribuidos (DDoS), se utilizan múltiples sistemas para aumentar el impacto del ataque.
- **Ejecución Remota de Código (RCE - Remote Code Execution)**: Vulnerabilidad que permite a un atacante ejecutar código malicioso en un servidor o sistema a distancia, lo que puede resultar en el control completo de la máquina afectada.
- **HSTS (HTTP Strict Transport Security)**: Es una política de seguridad web que fuerza a los navegadores a conectarse siempre a través de **HTTPS** y nunca permitir conexiones no seguras (HTTP). Protege contra ataques de intercepción (MITM).
- **HTTPS (Hypertext Transfer Protocol Secure)**: Protocolo que combina HTTP con SSL/TLS para cifrar la comunicación entre el navegador y el servidor web, asegurando que los datos transmitidos no puedan ser interceptados ni alterados.
- **ModSecurity**: Un firewall de aplicaciones web (WAF) de código abierto que proporciona detección y prevención de intrusiones para aplicaciones web. Se utiliza principalmente para mitigar ataques como inyecciones SQL y XSS.
- **Multifactor Authentication (MFA - Autenticación Multifactor)**: Proceso de autenticación que requiere dos o más pruebas de autenticación independientes para verificar la identidad de un usuario. Los factores pueden incluir algo que el usuario conoce (contraseña), algo que posee (token) o algo que es (biometría).

- **SCCP (Skinny Call Control Protocol)**: Protocolo utilizado por dispositivos Cisco IP Phones para establecer y gestionar sesiones de llamadas VoIP. Al ser un protocolo propietario, puede ser un objetivo común para ataques si no está configurado correctamente.
- **SIP (Session Initiation Protocol)**: Protocolo utilizado para establecer, modificar y finalizar sesiones multimedia en tiempo real, como llamadas de **VoIP**. Los servicios **SIP** son vulnerables a ataques de fuerza bruta si no están adecuadamente protegidos.
- **SIEM (Security Information and Event Management)**: Sistema que combina la gestión de información de seguridad (SIM) y la gestión de eventos de seguridad (SEM), permitiendo la recolección y análisis en tiempo real de eventos de seguridad, con el objetivo de detectar y responder rápidamente a incidentes de seguridad.
- **SMTP (Simple Mail Transfer Protocol)**: Protocolo estándar utilizado para la transmisión de correos electrónicos a través de redes IP. Si no está correctamente configurado, los servidores **SMTP** pueden ser explotados para el envío de spam o la fuga de información sensible.
- **STARTTLS**: Extensión de protocolos de correo electrónico como **SMTP** que permite que una conexión inicial no cifrada sea "actualizada" a una conexión cifrada utilizando **TLS**.
- **TLS (Transport Layer Security)**: Protocolo criptográfico que proporciona seguridad en las comunicaciones a través de redes. Es el sucesor de **SSL** y se utiliza para cifrar el tráfico en protocolos como **HTTPS**, **SMTP**, y **SIP**.
- **VoIP (Voice over Internet Protocol)**: Tecnología que permite realizar llamadas de voz utilizando una conexión a Internet en lugar de una línea telefónica convencional. **SIP** es uno de los protocolos más utilizados para la señalización en **VoIP**.
- **XSS (Cross-Site Scripting)**: Vulnerabilidad que permite a un atacante inyectar scripts maliciosos en sitios web legítimos. Estos scripts pueden ejecutarse en los navegadores de otros usuarios, permitiendo el robo de información o la suplantación de identidad.