UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:
PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA, Y/O DE DESARROLLO

TEMA:
ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD DE UNA MÁQUINA VIRTUAL CON FINES PRÁCTICOS: SERVIDOR WEB, SERVIDOR DE ARCHIVOS COMPARTIDOS, VULNERABILIDADES XSS Y GESTIÓN INCORRECTA DE PERMISOS

AUTORAS:
MARÍA JOSÉ CHÉVEZ MORÁN
JULISSA NICOLE MEDINA GRUEZO

DIRECTOR:
MIGUEL ARTURO ARCOS ARGUDO

CUENCA – ECUADOR
2024

Autoras:

María José Chévez Morán
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.

Julissa Nicole Medina Gruezo
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.

Dirigido por:

Miguel Arturo Arcos Argudo
Ingeniero de Sistemas.
Magíster en Seguridad de la Tecnologías de la Información y Comunicaciones.
Doctor en Ciencias de la Computación para Smart Cities.

Análisis de vulnerabilidades de seguridad de una máquina virtual con fines prácticos: Servidor WEB, Servidor de archivos compartidos, Vulnerabilidades XSS y gestión incorrecta de permisos

DEDICATORIA

Con profundo cariño y gratitud, dedico este proyecto a dos personas extraordinarias que han sido los pilares fundamentales en mi viaje hacia la maestría: mi querida abuelita Olimpia y mi amado esposo Jesús. Su apoyo incondicional desde el principio ha sido un recordatorio constante de la importancia de seguir mis sueños y perseguir mis metas con valentía y determinación.

A ambos les dedico este proyecto como un humilde homenaje a su inquebrantable fe en mí y a su constante apoyo a lo largo de esta travesía. Que este trabajo sea testimonio de mi profundo agradecimiento y amor hacia ustedes, mis queridos abuelita Olimpia y esposo Jesús, por ser mi inspiración y mi fuerza en este viaje hacia la realización académica y personal.

Julissa Medina Gruezo

Este proyecto está dedicado a mi mamá Holanda quien con su amor, paciencia y esfuerzo me ha permitido llegar a cumplir un sueño más, gracias por inculcar en mí el ejemplo del esfuerzo, de no rendirme porque Dios está conmigo siempre. Cada página escrita es un testimonio de tu dedicación y de la fe que has depositado en mí desde el primer día. Tú has sido mi guía en los momentos difíciles, mi inspiración en los momentos de duda y mi roca en medio de las tormentas. Este logro es el resultado de tus sacrificios, tus consejos y tu amor incondicional.

María José Chévez Morán

Agradecimiento

Quiero expresar mi más profundo agradecimiento a Dios, cuya guía constante y apoyo inquebrantable han sido los cimientos sobre los cuales se ha edificado este proyecto de tesis. Su presencia ha sido una fuente de fortaleza y dirección en cada etapa académica.

Además, quiero extender mi más sincero agradecimiento a mi familia y a mi esposo. Su apoyo incondicional, amor y comprensión han sido pilares indispensables en este largo camino hacia la maestría. Cada palabra de aliento, cada gesto de ánimo ha sido un faro de esperanza que me ha impulsado a superar los desafíos y a seguir adelante con determinación.

Por último, pero no menos importante, quiero expresar mi profunda gratitud a mi compañera de tesis, María José Chévez. Su colaboración constante, su valiosa contribución intelectual y su compañerismo inquebrantable fueron elementos esenciales para el éxito de este trabajo académico. Juntas hemos enfrentado los retos, celebrado los logros y compartido el peso de las responsabilidades, creando así un lazo de amistad y colaboración que trasciende las páginas de este documento.

Julissa Medina

Quiero dedicar un sincero agradecimiento a aquellos cuyo apoyo y presencia han sido pilares fundamentales en este viaje hacia la culminación de la maestría. A mi mamá, cuyo amor incondicional y sabiduría han sido una guía constante en cada paso de este camino. Tu paciencia y aliento han sido mi roca en los momentos de duda, y tu fe en mí ha sido mi mayor motivación. Gracias por ser mi inspiración y mi ejemplo de perseverancia.

A mis adorables sobrinos, cuya energía y alegría han iluminado incluso los días más difíciles de investigación y escritura. Su inocencia y cariño han sido un recordatorio constante de la importancia de este trabajo y de los sueños que persigo.

A mi querida compañera Julissa, por su constante apoyo, comprensión y ánimos en los momentos de desafío. Tu presencia ha sido un faro de luz en los momentos de oscuridad, y tu amistad ha sido un regalo invaluable en este viaje académico.

A todos aquellos que han contribuido de alguna manera a este logro, ya sea con palabras de aliento, consejos sabios o simplemente con su presencia amorosa, les doy las gracias de todo corazón. Este logro no habría sido posible sin su apoyo y amor incondicional.

María José Chévez Morán

Tabla de contenido

Contenido

Tabla de ilustraciones

ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD DE UNA MÁQUINA VIRTUAL CON FINES PRÁCTICOS: SERVIDOR WEB, SERVIDOR DE ARCHIVOS COMPARTIDOS, VULNERABILIDADES XSS Y GESTIÓN INCORRECTA DE PERMISOS

AUTOR(ES):

MARÍA JOSÉ CHÉVEZ MORÁN

JULISSA NICOLE MEDINA GRUEZO

Resumen

Este trabajo de titulación se centra en realizar una evaluación de las vulnerabilidades de seguridad que impactan en las máquinas virtuales, abordando de manera integral la seguridad de los servidores web y los servidores de archivos compartidos. Se destaca especialmente la amenaza significativa del Cross-Site Scripting (XSS), una preocupación crucial en los entornos web debido a su capacidad para infiltrar scripts maliciosos en páginas web, poniendo en riesgo la integridad de los datos y la seguridad de los usuarios.

Además de abordar esta problemática, se profundiza en otro desafío fundamental en materia de seguridad: la gestión inapropiada de permisos en los servidores de archivos compartidos. Una configuración incorrecta en este aspecto puede exponer datos altamente sensibles, comprometiendo tanto la privacidad como la seguridad de los usuarios y de la organización en su conjunto. Esta cuestión se relaciona estrechamente con el planteamiento anterior, donde se subrayó la importancia de una configuración adecuada de las máquinas virtuales para prevenir ataques y salvaguardar la integridad de la información.

El estudio lleva a cabo una exploración exhaustiva de las estrategias y mejores prácticas disponibles para evaluar y corregir estas configuraciones, realizando análisis y gestión de vulnerabilidades mediante el uso de herramientas especializadas en seguridad. El objetivo principal es garantizar la integridad de los datos y la seguridad de la experiencia del usuario. Este enfoque integral aborda la necesidad crítica de

realizar un análisis detallado y una configuración segura en el contexto de la virtualización.

En un entorno digital en constante evolución, con amenazas cibernéticas cada vez más sofisticadas, este estudio emerge como una herramienta esencial para proteger los activos digitales y asegurar la continuidad de las operaciones empresariales en entornos virtualizado. Su enfoque meticuloso y proactivo representa un paso significativo hacia la fortificación de la seguridad en un mundo digital cada vez más interconectado y expuesto a riesgos.

Palabras claves: vulnerabilidades, servidores, virtualización, Cross-Site Scripting, web

ABSTRACT

This degree project focuses on carrying out an assessment of the security vulnerabilities that impact virtual machines, comprehensively addressing the security of web servers and shared file servers. The significant threat of Cross-Site Scripting (XSS) is especially highlighted, a crucial concern in web environments due to its ability to infiltrate malicious scripts into web pages, putting data integrity and user security at risk.

In addition to addressing this problem, it delves into another fundamental security challenge: the inappropriate management of permissions on shared file servers. An incorrect configuration in this aspect can expose highly sensitive data, compromising both the privacy and security of users and the organization as a whole. This issue is closely related to the previous approach, where the importance of proper configuration of virtual machines was stressed to prevent attacks and safeguard the integrity of information.

The study carries out an exhaustive exploration of the strategies and best practices available to evaluate and correct these configurations, performing analysis and vulnerability management through the use of specialized security tools. The main objective is to ensure the integrity of the data and the security of the user experience. This comprehensive approach addresses the critical need for detailed analysis and secure configuration in the context of virtualization.

In a constantly evolving digital environment, with increasingly sophisticated cyber threats, this study emerges as an essential tool to protect digital assets and ensure the continuity of business operations in virtualized environments. His meticulous and proactive approach represents a significant step towards fortifying security in an increasingly interconnected and risk-exposed digital world.

Keywords: Vulnerabilities, servers, virtualization, Cross-Site Scripting, web

1. Introducción

En la actualidad, el agigantado progreso tecnológico y la incorporación de diversas innovaciones han impulsado a corporaciones e instituciones de todo ámbito a buscar una optimización exhaustiva de sus recursos y procesos, con el fin elevar los estándares de producción. En el pasado, la idea de optimizar procesos conllevaba una utilización considerable de recursos físicos en el ámbito tecnológico; y este enfoque no solo implicaba una creciente demanda de hardware, sino que también acarreaba consigo una serie de desafíos y costos significativos. La expansión de infraestructura tecnológica en ese entonces resultaba en inversiones considerables tanto en términos de infraestructura, mantenimiento y reparaciones puesto que la adquisición de mayor cantidad de hardware generaba gastos adicionales asociados a espacio físico, actualización, reparación, y sustitución de hardware. Como solución a la problemática mencionada surgió la virtualización. ¿De qué se trata la virtualización? De acuerdo con Luis Joyanes Aguilar, la virtualización se refiere a la abstracción de los recursos de computación como CPU, almacenamiento, redes, memoria, sistemas operativos, aplicaciones, base de datos, etc. Mediante la virtualización un servidor físico se puede dividir en varios servidores virtuales, cada uno con sistema operativo y recursos propios [1]. Pero la virtualización no es una innovación reciente, ya que tiene una trayectoria de aproximadamente cinco décadas. El origen de la virtualización se puede encontrar en varios proyectos en los que se destaca el proyecto Atlas llevado a cabo por la Universidad de Manchester. Atlas, un supercomputador que comenzó a operar en 1962,

fue uno de los primeros en implementar técnicas de virtualización con el objetivo de crear múltiples máquinas virtuales que ejecutaran diversos procesos de manera aislada en un mismo hardware. Este hito representó una revolución en la capacidad de procesamiento y la eficaz utilización de los recursos computacionales [2].

La virtualización permite que varias máquinas virtuales se ejecuten en simultáneo con distintos sistemas operativos y recursos propios, aunque físicamente solo sea un equipo. Una máquina virtual es un contenedor de software totalmente aislado y capaz de ejecutar sistemas operativos y aplicaciones propios como si fuere un ordenador físico [3]. En este contexto, elementos cruciales como la memoria RAM, las unidades de procesamiento (CPU), los discos duros, entre otros, se transforman en recursos disponibles para las máquinas virtuales, permitiendo un aprovechamiento eficiente y compartido de dichos recursos. Además, la virtualización ofrece flexibilidad al permitir la rápida creación, replicación y migración de máquinas virtuales, brindando así una adaptabilidad dinámica a las cambiantes necesidades del entorno informático.

A medida que las tecnologías evolucionan para abordar y contribuir en la resolución de diversas problemáticas, los avances en tácticas fraudulentas y estudios de ataques informáticos también progresan de manera notable. Las máquinas virtuales al ser portadoras de gran cantidad de información y procesos en la actualidad se convierten en blancos de gran relevancia para posibles amenazas y ataques cibernéticos. Este escenario destaca la importancia crítica de fortalecer la seguridad en entornos virtuales, dado que su vulnerabilidad potencial puede representar una seria amenaza para la integridad y confidencialidad de la información.

Es crucial tener presente que, al crear y administrar máquinas virtuales, estas se convierten en objetivos constantes de ataques cibernéticos. Por ende, es de suma importancia estudiar minuciosamente las posibles vulnerabilidades que podrían afectar a las máquinas virtuales y tener un meticuloso cuidado en la gestión de permisos. En cuanto a vulnerabilidades es importante conocer los riesgos de las vulnerabilidades Cross-Site Scripting (XSS); Según Chalabe Nasser, XSS es una forma de ataque de inyección de scripts que ocurre en aplicaciones web, donde se asume el control del navegador del usuario para ejecutar códigos maliciosos o scripts. Esta vulnerabilidad

suele ser aprovechada cuando los datos de entrada utilizados en las aplicaciones no se validan adecuadamente, lo que permite enviar un script malicioso a la aplicación [4].

La gestión de permisos es un procedimiento fundamental en la administración de sistemas, ya que es el proceso en el que se define que los usuarios dispongan de un nivel adecuado de acceso a sistemas críticos. En resumen, los permisos de usuarios se definen como un conjunto de normativas que determinan las acciones que los usuarios están autorizados o prohibidos a llevar a cabo dentro de un sistema [5].

Nuestro estudio se centra en el núcleo de la seguridad informática, abordando aspectos críticos como servidores web, servidores de archivos compartidos, vulnerabilidades XSS (Cross-Site Scripting, que permiten la inserción de scripts maliciosos en páginas web) y la gestión incorrecta de permisos, la cual puede generar brechas significativas en la seguridad. El objetivo primordial de este análisis es proporcionar a usuarios, gestores y administradores de máquinas virtuales las herramientas necesarias para identificar, evaluar y abordar de manera efectiva amenazas como las vulnerabilidades XSS y la gestión incorrecta de permisos en entornos de máquinas virtuales que funcionan como servidores web y servidores de archivos compartidos. Esta aproximación fortalece la seguridad y resguarda la integridad de sistemas críticos en un entorno cada vez más interconectado y susceptible a los ataques de ciberdelincuentes.

2. Determinación del problema

En el contexto del continuo crecimiento de la virtualización, se ha observado un incremento significativo en los ciberataques dirigidos a las máquinas virtuales. A pesar de las innegables ventajas que ofrecen las máquinas virtuales, también presentan vulnerabilidades particulares que los ciberdelincuentes pueden aprovechar con fines maliciosos. Un aspecto crítico que merece atención es la capacidad de restaurar una máquina virtual a un estado anterior, una función que, si no se gestiona adecuadamente, puede dar lugar a la reintroducción de vulnerabilidades previamente abordadas, como parches de programas obsoletos, servicios desactivados y contraseñas antiguas. La problemática radica en que la facultad de revertir una máquina virtual a un estado anterior, aunque valiosa para la gestión y recuperación de sistemas, también puede ser explotada con propósitos maliciosos. Esto otorga a los atacantes la posibilidad de reproducir ataques anteriores y eludir cualquier protocolo de seguridad basado en el estado actual de la máquina.

Un ejemplo reciente de esta problemática se evidenció en el ataque a la compañía IFX Networks, donde los atacantes bloquearon el acceso a los sistemas de la empresa y cifraron la información. Además, aprovecharon la capacidad de restauración de máquinas virtuales para mantener el control sobre la infraestructura de red

comprometida. Este incidente afectó a más de 700 máquinas, incluyendo servidores físicos y virtuales, resultando en una grave pérdida de datos y representando una amenaza significativa para la confidencialidad de la información de los clientes [6].

En vista de este contexto, se vuelve evidente la necesidad de llevar a cabo un análisis para la creación y configuración segura de máquinas virtuales. Esto implica no solo considerar la eficiencia operativa, sino también tener en cuenta los parámetros de seguridad que prevengan la explotación de vulnerabilidades y reduzcan el riesgo de ciberataques capaces de comprometer la integridad de la información y la continuidad del negocio.

Reconocida la relevancia de las vulnerabilidades descritas en la sección anterior, se puede definir el problema como los persistentes ataques a máquinas virtuales y la explotación de vulnerabilidades XSS y permisos incorrectos. Este problema será abordado en el proyecto mediante el diseño, la configuración y la implementación de una máquina virtual que, de manera deliberada, incluya vulnerabilidades asociadas a un servidor web, servidor de archivos compartidos, vulnerabilidades XSS y una gestión incorrecta de permisos.

3. Marco teórico referencial

Una **máquina virtual**, es una entidad independiente que representa un sistema operativo y una o varias aplicaciones, ejecutándose en un entorno virtualizado donde su ejecución se materializa en un host, capitalizando una porción estratégica de los recursos hardware disponibles para su funcionamiento óptimo [7]. En este entorno dinámico, cada máquina virtual tiene una asignación personalizada de recursos virtuales, tales como capacidad de procesamiento (CPU), memoria, espacio de almacenamiento y capacidades de red. Los recursos se asignan de acuerdo con las necesidades, desde el nivel físico hasta las máquinas virtuales (VM). Al simular y reproducir las funciones de una máquina física, la máquina virtual es, capaz de albergar y ejecutar sistemas operativos completos junto con sus respectivas aplicaciones. Para la gestión de las máquinas virtuales se requiere de un hipervisor que la gestión del hardware del sistema y separa los recursos físicos en distintos entornos virtuales.

Un **hipervisor** es un software que se instala sobre hardware, creando una capa de virtualización y actuando como una plataforma en la que se crean las VM. El hipervisor gestiona todos los recursos físicos del sistema host, como CPU, memoria, red y almacenamiento. Los hipervisores simplifican la gestión de recursos, aceleran la implementación, utilizan los recursos de manera más eficiente y ofrecen un mejor control sobre la infraestructura [8]. Los Hipervisores se clasifican en dos tipos: tipo 1 (virtualización bare metal), se instalan directamente en el hardware del servidor y tipo 2 (virtualización alojada), se instalan en el sistema operativo anfitrión del usuario [9].

El hipervisor de Tipo 1 se instala directamente sobre el hardware, se le conoce como hipervisor de metal desnudo (bare metal hypervisor). El software del hipervisor está literalmente instalado sobre el hardware de metal. Con un hipervisor de Tipo 1, un equipo puede ejecutar un sistema operativo (por ejemplo, Windows) y también una o más instancias de otro sistema operativo como Linux Ubuntu, o una versión anterior de Windows [10].

Hipervisor de Tipo 2, también denominado hipervisor alojado, se instala sobre el sistema operativo existente y no sobre el hardware como en el caso del hipervisor de metal desnudo. El hipervisor alojado depende del sistema operativo host para proporcionar acceso directo a los recursos de hardware del equipo y administrar esos recursos para crear máquinas virtuales [10]. La mayor ventaja del hipervisor de Tipo 2 es que es muy fácil de descargar y permite empezar a explorar la virtualización creando máquinas virtuales propias.

Un **programa de servidor basado en software** es una aplicación que proporciona un servicio específico que otros programas, conocidos como clientes, pueden utilizar de manera local o a través de una red. El tipo de servicio ofrecido por el servidor está determinado por la naturaleza del software que lo compone. La comunicación se fundamenta en el modelo cliente-servidor, y para la transferencia de datos se utilizan protocolos de transmisión específicos del servicio en cuestión [11]. Desempeñan un papel crucial al almacenar y garantizar la disponibilidad constante y segura del contenido en Internet. Cuando se accede a una página web a través del navegador, en realidad, un servidor web transmite los componentes individuales de esa página directamente al dispositivo.

Cada página web accesible en Internet requiere un servidor especializado para alojar sus contenidos web. En muchas ocasiones, las grandes empresas y organizaciones disponen de su propio servidor web para gestionar sus contenidos tanto en Intranet como en Internet. Sin embargo, la mayoría de los administradores optan por utilizar los centros de datos proporcionados por proveedores de alojamiento web para sus proyectos. Ya sea que se posea un servidor web propio o alquilado a un tercero, siempre será necesario contar con software que gestione los datos de la página y los mantenga actualizados. Este servidor permite que las páginas, imágenes y videos puedan ser publicadas y

distribuidas en internet, además permite dar crecimientos a aplicaciones basadas en http [12].

Un **servidor de archivos** es un componente clave de una red informática, ya que proporciona almacenamiento centralizado para los archivos de los dispositivos de datos de los usuarios. El administrador del servidor establece reglas de acceso para determinar quién puede ver y manipular los archivos. Además del acceso a través de la red local, cuando el servidor de archivos está conectado a Internet, también permite el acceso remoto, lo que permite a los usuarios ubicados en diferentes lugares acceder a los archivos almacenados en el servidor. Los servidores de archivos son compatibles con diferentes sistemas operativos, como Windows, Linux o macOS, siempre que sean compatibles con los dispositivos de la red. Además de almacenar y gestionar archivos, el servidor de archivos puede utilizarse también como servidor de copias de seguridad o como repositorio de programas que deben estar disponibles para varios usuarios de la red [13].

Un **servidor virtual** opera de manera similar a un servidor físico, pero la tecnología de virtualización permite separar sus recursos del entorno físico. Cada servidor virtual tiene la capacidad de ejecutar su propio sistema operativo, aplicaciones y cargas de trabajo de manera independiente sin interferir con los demás recursos del sistema central. La virtualización de servidores optimiza la utilización de la capacidad del servidor de manera más eficiente, lo que a su vez aumenta la productividad al permitir que los usuarios accedan a los datos de manera segura y eficaz. Además, la virtualización desempeña un papel fundamental en la preservación de los recursos informáticos, centraliza la administración de servidores y elimina el sobre aprovisionamiento de recursos. Y, en este punto ya se infiere de una arquitectura mayor, si tomamos en cuenta que se desea tener de forma inmediata, transparente y digitalizada [14].

Las vulnerabilidades conocidas como ataques **Cross-Site Scripting (XSS)** se hallan comúnmente en aplicaciones web, manifestándose mediante la inyección de código en el lado del cliente mediante la inclusión de un archivo. Estos ataques XSS tienen el potencial de manipular y exponer datos confidenciales. Uno de los métodos más prevalentes implica acceder a sesiones o sustraer cookies, permitiendo así la recopilación de información confidencial [15] . Este tipo de ataque se lleva a cabo

principalmente en dos etapas. En la primera fase, el atacante busca inducir a la víctima a hacer clic en una ubicación predeterminada o cargar una página web, generalmente utilizando técnicas de ingeniería social a través de enlaces maliciosos. La segunda fase implica el envío de la solicitud desde el navegador de la máquina víctima (cliente) al servidor, de tal manera que la acción parezca inofensiva para la víctima. Principalmente existen 3 tipos de ataques XSS:

***XSS persistente o almacenado**:* Este tipo se destaca como la variante más perjudicial y riesgosa de las formas de XSS mencionadas en el documento. La inyección de este código queda almacenada en el servidor, lo que implica que cada vez que cualquier usuario visite la página con el código inyectado, se ejecutará, dando lugar a la realización de acciones no deseadas por parte del usuario [16].

XSS no persistente o reflejado: A diferencia del XSS persistente, la inyección de este código no queda almacenada en el servidor, pero permite que se ejecuten acciones en el lado del cliente, generando así resultados no deseados [16].

XSS basado en DOM: Este tipo de ataque XSS se presenta de manera ligeramente diferente a los mencionados anteriormente, ya que se manifiesta en el DOM (Document Object Model) en lugar de hacerlo en el lenguaje HTML [16].

4. Metodología y desarrollo

Para la ejecución de la presente investigación, se procede con la adaptación de un caso de estudio para la ejemplificación de los conceptos. En este contexto, se ha concebido un proceso de desarrollo que consiste en la creación y configuración de una máquina virtual, la cual actúa como servidor web y de archivos compartidos, dotada de vulnerabilidades de tipo XSS (Cross-Site Scripting) y una gestión de permisos susceptible a fallos. Los objetivos delineados para este proyecto comprenden la elaboración del estado del arte, la configuración meticulosa del servidor virtual en cuestión, la ejecución de un análisis detallado de las vulnerabilidades presentes y, finalmente, la implementación de medidas correctivas destinadas a mitigar dichas vulnerabilidades identificadas durante el proceso de investigación.

4.1 Breve reseña histórica (Estado de arte)

Máquinas virtuales

Las máquinas virtuales tuvieron sus inicios en la década de los 60, cuando IBM introdujo las primeras durante el lanzamiento del mainframe IBM S/360 Modelo 67, diseñado específicamente para la virtualización. Esta innovación permitía la ejecución simultánea de múltiples sistemas operativos en una sola infraestructura hardware, marcando un cambio significativo en la arquitectura informática [17].

En 1960 desarrollado por Martin Richards apareció el lenguaje BCPL (Basic Combined Programming Language), en el que se basa el lenguaje C, con un código intermedio llamado O-code que podía interpretarse como una máquina virtual o compilarse para la máquina nativa, impulsando la portabilidad y popularidad del lenguaje [17].

En la década de 1970, en la Universidad de California en San Diego, se adoptó el p-code, un enfoque de máquina virtual para ejecutar Pascal compilado, buscando simplificar el desarrollo del compilador Pascal al lograr independencia del hardware [17].

En 1972, Xerox PARC introdujo Smalltalk, un lenguaje que dependía de una máquina virtual para su ejecución. P-code y Smalltalk influyeron en la creación de uno de los lenguajes más influyentes basados en máquina virtual: Java, concebido por Sun Microsystems en 1985, que materializó la idea de una programación independiente de la plataforma mediante la Java Virtual Machine [17].

Durante las décadas de 1980 y 1990, la arquitectura x86 se consolidó como fuerza impulsora en la tecnología, pero su adopción provocó desafíos como costos de infraestructura y protección contra fallos, lo que llevó a una reevaluación de la virtualización como estrategia informática [18].

En 1998, un grupo de investigadores de la Universidad de California fundó VMware con el propósito de abordar las deficiencias en la arquitectura x86, marcando otro hito en la evolución de las máquinas virtuales.

Cross-Site Scripting XSS

El origen de las vulnerabilidades XSS se remonta a 1996 en los primeros años de la World Wide Web (WWW), cuando el e-commerce empezaba a despuntar. Cuando miles de páginas estaban bajo construcción y usaban HTML. Apareció JavaScript brindando a los desarrolladores la capacidad de diseñar sitios web interactivos repletos de efectos impresionantes. Sin embargo, los hackers exploraron un ámbito completamente nuevo de oportunidades. Ellos aprovecharon la capacidad de JavaScript para cargar otros sitios web dentro de un navegador robando datos sensibles. En 1999, David Ross identificó estas vulnerabilidades en Internet Explorer, dando origen al término "Cross-Site Scripting" (XSS) [19].

4.2 Materiales

En esta sección se describirá brevemente las herramientas utilizadas para el desarrollo del presente trabajo.

VMWare Workstation: Es un software de virtualización de escritorio que permite a los usuarios ejecutar múltiples sistemas operativos como máquinas virtuales (VMs) en una única computadora física. Diseñado para desarrolladores y profesionales de TI, VMware Workstation proporciona una plataforma para probar, desarrollar, demostrar y desplegar software simulando diversos entornos de computación en un entorno seguro y aislado [20]**.** Entre las características que nos ofrece VMware Workstation se encuentra su compatibilidad con casi todas las versiones de Windows, Linux y otros sistemas operativos como invitados. Además, incluye la función de Snapshots, que permite a los usuarios guardar el estado completo de una máquina virtual en cualquier momento, facilitando así la restauración a un estado anterior sin necesidad de reinstalar el sistema operativo.

S.O. Ubuntu: Ubuntu, un sistema operativo de código abierto basado en Linux y fundamentado en Debian, abarca una amplia gama de versiones que se adaptan a diversas necesidades. Estas variantes comprenden Ubuntu Desktop, Cloud, Phone, Tablet y Server [21]. El patrocinio de este sistema operativo proviene de Canonical Ltd., una entidad empresarial privada financiada por el empresario sudafricano Mark Shuttleworth [22]. Es importante destacar que el software de Ubuntu Server se presenta sin entorno gráfico, limitándose únicamente a líneas de comando, con el propósito de optimizar el uso de recursos del servidor para su función principal. [21]

XAMPP v7.4: Es una distribución de software libre desarrollada por Apache Friends bajo la licencia GNU General Public License (GPL). Esta distribución incluye una serie de herramientas y aplicaciones esenciales para el desarrollo web y la gestión de bases de datos. Entre los componentes destacados se encuentran el servidor web Apache, el sistema de gestión de bases de datos MySQL o MariaDB, el intérprete de scripting PHP y el lenguaje de programación Perl [23]. El nombre "XAMPP" es un acrónimo que representa las iniciales de los componentes que lo constituyen: X para "cualquier sistema operativo", A para Apache, M para MySQL/MariaDB, P para PHP y el segundo P para Perl.

Esta combinación de tecnologías es ampliamente utilizada en el desarrollo web y proporciona un entorno robusto y flexible para la creación de aplicaciones y sitios web dinámicos [23].

Samba: Es una suite de aplicaciones Unix que se fundamenta en el protocolo SMB (Server Message Block), el cual goza de amplio uso en sistemas operativos diversos, como Windows y otras plataformas basadas en Unix. Su principal función radica en agilizar las operaciones cliente-servidor en redes [24]. La versatilidad de SAMBA se refleja en su capacidad para funcionar en una amplia gama de sistemas Unix, incluidas distribuciones de GNU/Linux, Solaris y las distintas variantes de BSD incluso Mac OS X Server. Esta compatibilidad multiplataforma permite a los usuarios compartir archivos e impresoras de manera eficiente [24].

Qualys: Se trata de una solución de seguridad en la nube empleada para el manejo de vulnerabilidades y el cumplimiento de políticas de seguridad en empresas de diversas dimensiones. Este sistema asiste a los equipos de seguridad en la detección y corrección de vulnerabilidades en tiempo real, asegurando la integridad de la infraestructura de tecnologías de la información (TI) [25]. Qualys proporciona una variedad extensa de herramientas destinadas a asegurar la seguridad en redes. Estas incluyen funciones como la detección de amenazas, la administración de actualizaciones, la evaluación de vulnerabilidades y el cumplimiento de normativas. La versatilidad de Qualys permite su adaptación a los requerimientos de seguridad de cualquier entidad, además de su alta escalabilidad.

4.3 Metodología

Para llevar a cabo este estudio, se implementa un enfoque metodológico que combina elementos deductivos y exploratorios, centrándose en la investigación de conceptos relacionados con la virtualización, la creación de máquinas virtuales y el posterior análisis de sus vulnerabilidades.

Luego de la presentación del marco teórico, se ha procedido con la creación de máquinas virtuales, introduciendo configuraciones erróneas de manera intencionada. Esto permitirá simular situaciones que podrían llevar a vulnerabilidades en las máquinas virtuales y, de esta manera, facilitar el análisis de sus debilidades.

Posteriormente, se ha llevado a cabo un minucioso escaneo de vulnerabilidades utilizando herramientas y técnicas especializadas. Este proceso tiene como objetivo identificar y documentar cualquier vulnerabilidad existente en las máquinas virtuales creadas previamente.

Finalmente, se ha consolidado los hallazgos en un detallado manual que contiene información sobre las vulnerabilidades descubiertas. Este manual servirá como una valiosa referencia para futuras creaciones de máquinas virtuales, brindando pautas específicas para evitar y abordar vulnerabilidades, y así fortalecer la seguridad en entornos virtuales.

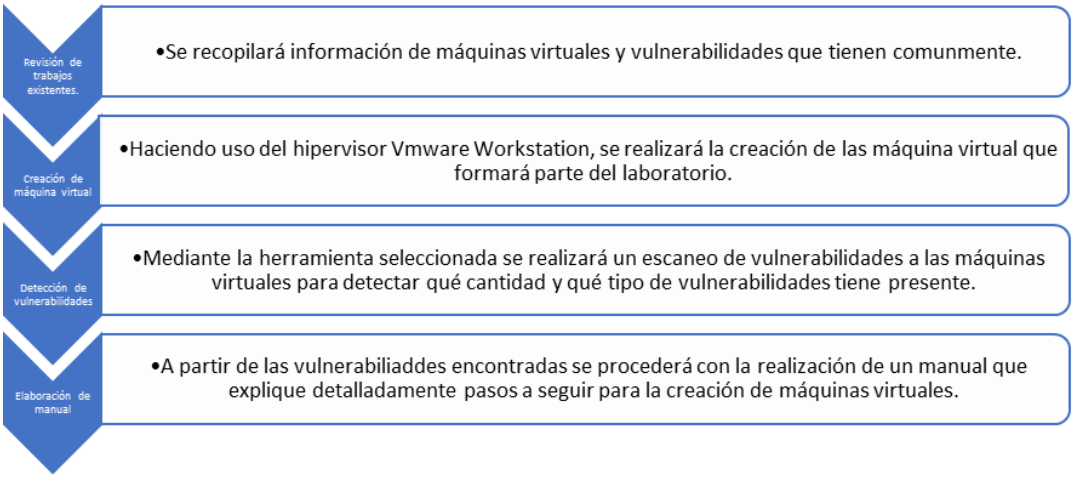


Ilustración 1- Metodología

4.4 Desarrollo

1. **Objetivo del Laboratorio**

El objetivo del laboratorio con configuraciones incorrectas en Ubuntu Server es proporcionar a los usuarios una experiencia práctica en la identificación y solución de problemas derivados de configuraciones erróneas en un entorno de servidor Linux. Al enfrentarse a situaciones simuladas de configuración incorrecta, los usuarios pueden aprender a reconocer errores comunes, diagnosticar problemas y aplicar soluciones para restaurar el funcionamiento adecuado del sistema. Este enfoque práctico fomenta el aprendizaje activo y fortalece las habilidades de administración de sistemas en entornos Linux. Las configuraciones se realizaron con la revisión de artículos académicos y videos.

2. **Requisitos previos**

- Instalar Vmware Workstation

- Imagen ISO de Ubuntu Server: https://ubuntu.com/download/server
- Para este laboratorio se usarán los siguientes requisitos:
  - 4 núcleos vCPU
  - 8gb RAM
  - 200gb HDD
  - NIC en modo bridge

Configuración del servidor

Para iniciar la configuración del servidor instalamos VMware Workstation:

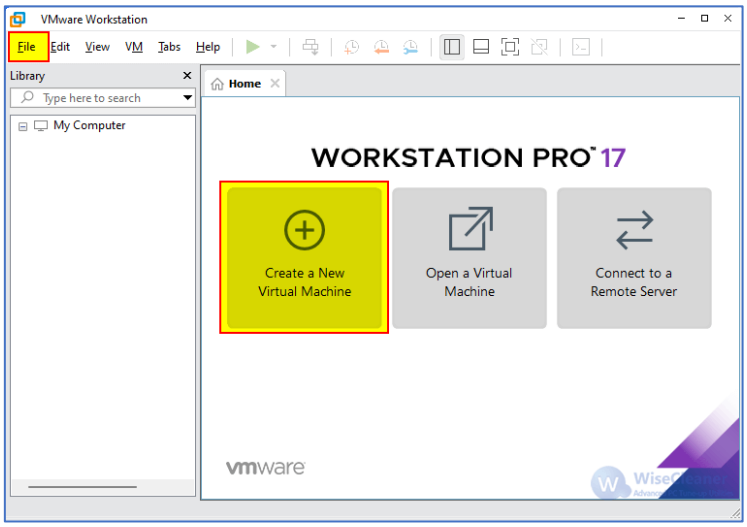


Ilustración 2 - Entorno de VMware Workstation

Instalación de Ubuntu Server sin parches

La versión que se usa es **Ubuntu server 22.04**, para ello se crea la máquina virtual dentro de la herramienta y se asignan los recursos mencionados.

Utilizar Ubuntu Server 22.04 sin aplicar parches de seguridad permite experimentar con un sistema operativo en un estado vulnerable. Esto reproduce condiciones realistas que podrían encontrarse en escenarios de producción debido a la desactualización o malas prácticas de mantenimiento.

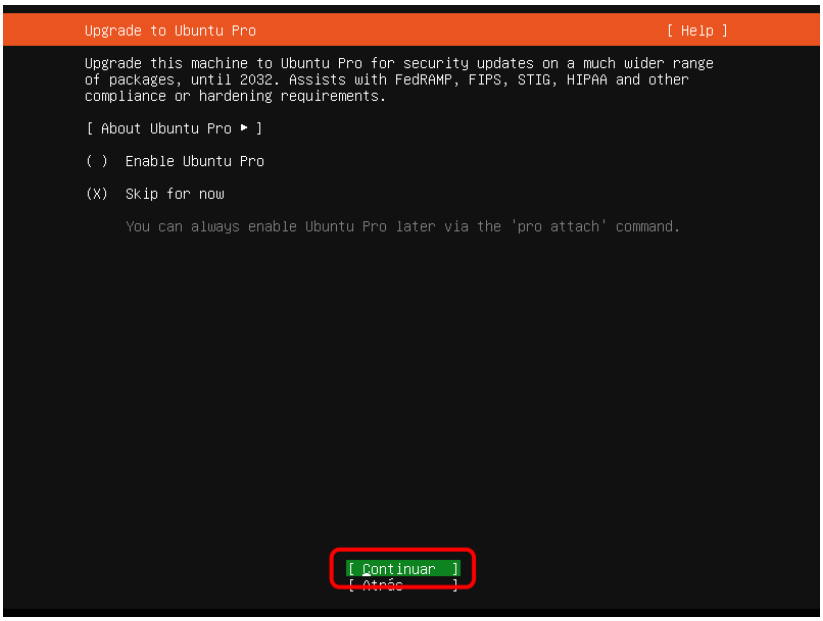


Ilustración 3 - Ubuntu sin parches

Las demás configuraciones se dejan por default y se finaliza la instalación.

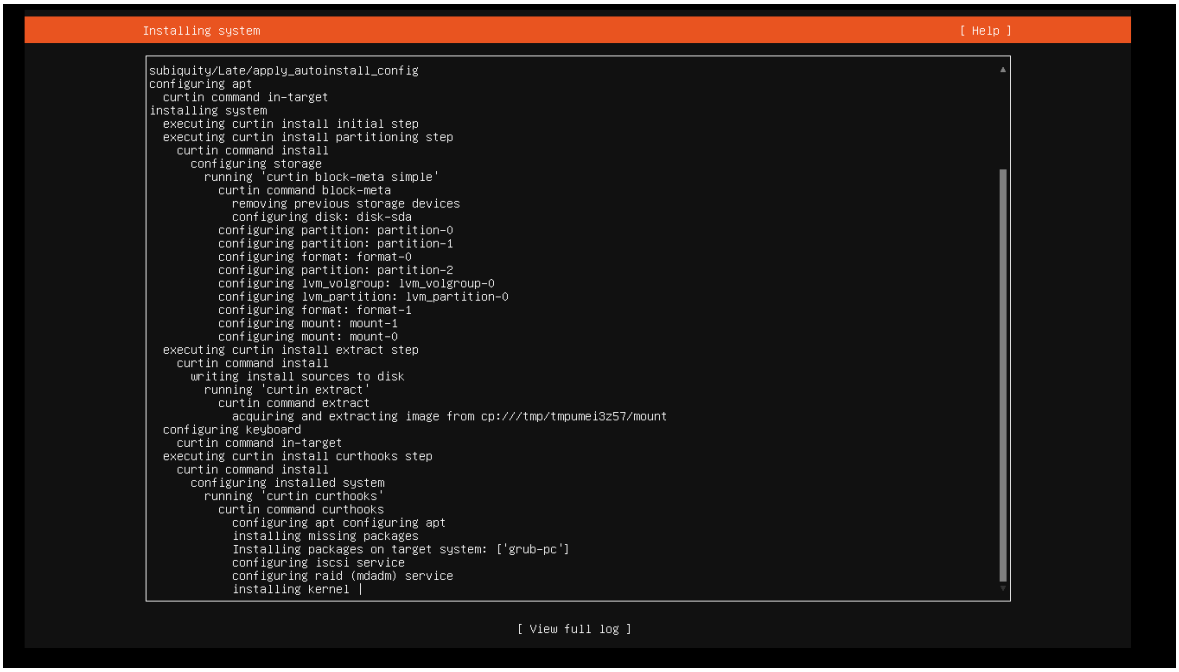


Ilustración 4 - Finalización de instalación de UBUNTU SERVER

Para tener una configuración estable se debe establecer una ip estática en el server, para ello se hará uso de la herramienta VIM para editar el archivo de configuración de netplan el cual contiene los datos de la NIC de DHCP a estático.

Se usa el comando:

vim /etc/netplan/00-installer-config.yaml

```
webadmin@lab4:~$
webadmin@lab4:~$
webadmin@lab4:~$
webadmin@lab4:~$
webadmin@lab4:~$
webadmin@lab4:~$ vim /etc/netplan/00-installer-config.yaml _
```

Ilustración 5 - Configuración de IP estática

Se guarda el archivo y se aplican los cambios con el comando:

netplan apply

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
      addresses: [192.168.1.90/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8]
  version: 2
```

Ilustración 6 - Archivo editado netplan con IP estática

```
root@lab4:~# netplan apply

** (generate:1991): WARNING **: 07:06:04.484: `gateway4` has been deprecated, use default routes ins
tead.
See the 'Default routes' section of the documentation for more details.
WARNING:root:Cannot call Open vSwitch: ovsdb-server.service is not running.

** (process:1989): WARNING **: 07:06:04.859: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:1989): WARNING **: 07:06:05.187: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:1989): WARNING **: 07:06:05.188: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.
root@lab4:~# _
```

Ilustración 7 - Cambios Aplicados.

El equipo está preparado para llevar a cabo la instalación y configuración del servidor web.

WEBSERVER

Se utiliza la herramienta WGET, la cual permite descargar el instalador desde el sitio de XAMPP.

Se usa el comando:

Wget https://www.apachefriends.org/xampp-files/7.4.33/xampp-linux-x64-7.4.33-0-installer.run

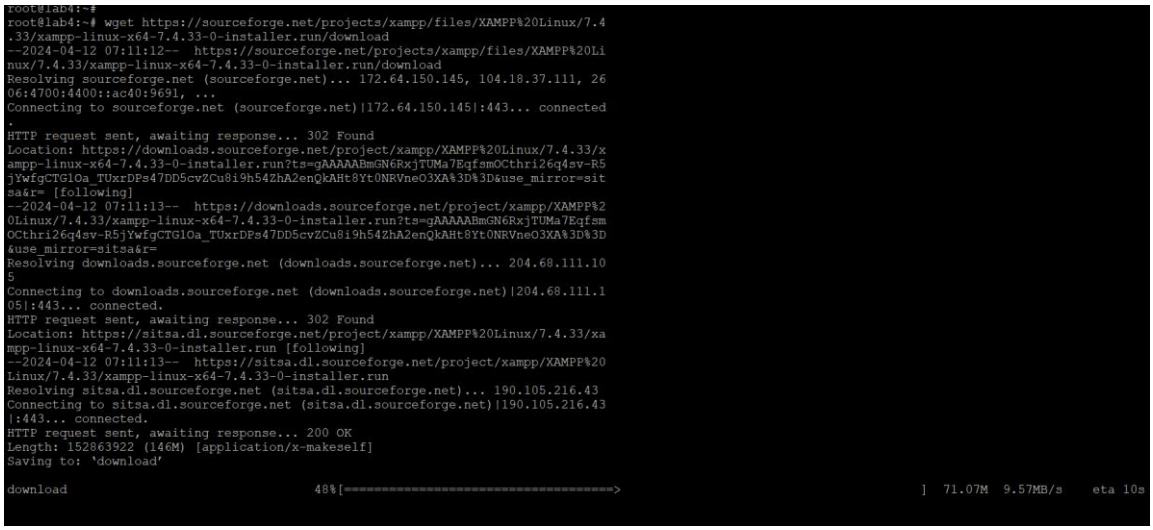


Ilustración 8 - Descarga de XAMPP con WGET

Se cambian los permisos del archivo descargado con el fin de no tener errores en la instalación, con el comando:

Sudo chmod +x xampp-linux-*-installer.run

```
root@lab4:~#
root@lab4:~# chmod +x xampp-linux-*-installer.run
root@lab4:~#
root@lab4:~#
root@lab4:~# ls -la
total 149316
drwx------  4 root root      4096 Apr 12 07:17  .
drwxr-xr-x 20 root root      4096 Apr 12 06:40  ..
-rw-r--r--  1 root root      3106 Oct 15  2021  .bashrc
-rw-r--r--  1 root root       161 Jul  9  2019  .profile
drwx------  3 root root      4096 Apr 12 06:45  snap
drwx------  2 root root      4096 Apr 12 06:45  .ssh
-rw-------  1 root root      1026 Apr 12 07:05  .viminfo
-rw-r--r--  1 root root       170 Apr 12 07:11  .wget-hsts
-rwxr-xr-x  1 root root 152863922 Nov 22  2022 'xampp-linux-*-installer.run'
root@lab4:~#
root@lab4:~#
root@lab4:~#
```

Ilustración 9- Cambio de permisos

Se procede a realizar la instalación con el comando:

Sudo ./xampp-linux-*-installer.run

```
root@lab4:~#
root@lab4:~# ./xampp-linux-*-installer.run
--------------------------------------------------------------------------
Welcome to the XAMPP Setup Wizard.

--------------------------------------------------------------------------
Select the components you want to install; clear the components you do not want
to install. Click Next when you are ready to continue.

XAMPP Core Files : Y (Cannot be edited)

XAMPP Developer Files [Y/n] :y

Is the selection above correct? [Y/n]: y

--------------------------------------------------------------------------
Installation Directory

XAMPP will be installed to /opt/lampp
Press [Enter] to continue:y

--------------------------------------------------------------------------
Setup is now ready to begin installing XAMPP on your computer.

Do you want to continue? [Y/n]: y

--------------------------------------------------------------------------
Please wait while Setup installs XAMPP on your computer.

 Installing
 0% _____________ 50% _____________ 100%
 ###
```

Ilustración 10 - Proceso de instalación XAMPP

Una vez finalizada la instalación se debe inicializar los servicios de xampp, con el comando:

sudo /opt/lampp/lampp start

```
root@lab4:~# sudo /opt/lampp/lampp start
Starting XAMPP for Linux 7.4.33-0...
XAMPP: Starting Apache...already running.
XAMPP: Starting MySQL.../opt/lampp/share/xampp/xampplib: line 22: netstat: command not found
ok.
XAMPP: Starting ProFTPD.../opt/lampp/share/xampp/xampplib: line 22: netstat: command not found
ok.
root@lab4:~#
```

Ilustración 11 - Validación que los servicios están corriendo

Así mismo procedemos a la validación a través del navegador.

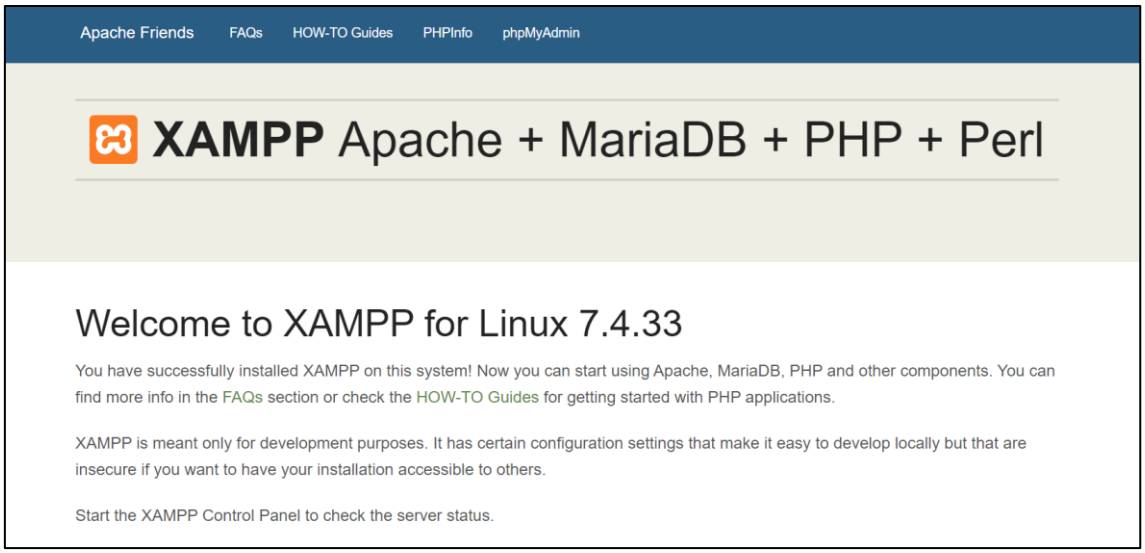


Ilustración 12 - Validación de servicios corriendo en navegador

Finaliza instalación del web server.

FILESERVER

Para configurar el servicio de archivos compartidos en el servidor se usará samba, esta herramienta permitirá compartir archivos desde Linux.

Se instala con el comando:

apt install samba

```
root@lab4:~#
root@lab4:~# apt install samba
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr ibverbs-providers libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcups2
  libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1 libldb2 libnl-route-3-200 librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-pygments python3-requests-toolbelt python3-samba python3-talloc
  python3-tdb samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
Suggested packages:
  cups-common python3-sniffio python3-trio python-markdown-doc python-pygments-doc ttf-bitstream-vera bind9 bind9utils ctdb ldb-tools ntp | chrony
  smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcups2
  libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1 libldb2 libnl-route-3-200 librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 liburing2
  libwbclient0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-pygments python3-requests-toolbelt python3-samba python3-talloc
  python3-tdb samba samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
0 upgraded, 39 newly installed, 0 to remove and 17 not upgraded.
Need to get 20.1 MB of archives.
After this operation, 106 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 libtalloc2 amd64 2.3.3-2build1 [25.6 kB]
Get:2 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 libtevent0 amd64 0.11.0-1build1 [39.2 kB]
Get:3 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libwbclient0 amd64 2:4.15.13+dfsg-0ubuntu1.6 [266 kB]
Get:4 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 python3-dnspython all 2.1.0-1ubuntu1 [123 kB]
Get:5 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 libtdb1 amd64 1.4.5-2build1 [46.4 kB]
Get:6 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libldb2 amd64 2:2.4.4-0ubuntu0.22.04.2 [154 kB]
Get:7 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3-ldb amd64 2:2.4.4-0ubuntu0.22.04.2 [41.7 kB]
Get:8 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 python3-tdb amd64 1.4.5-2build1 [15.5 kB]
Get:9 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libavahi-common-data amd64 0.8-5ubuntu5.2 [23.8 kB]
Get:10 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libavahi-common3 amd64 0.8-5ubuntu5.2 [23.9 kB]
Get:11 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libavahi-client3 amd64 0.8-5ubuntu5.2 [28.0 kB]
Get:12 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcups2 amd64 2.4.1op1-1ubuntu4.8 [264 kB]
Get:13 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 python3-talloc amd64 2.3.3-2build1 [13.0 kB]
Get:14 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 samba-libs amd64 2:4.15.13+dfsg-0ubuntu1.6 [6,276 kB]
Get:15 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 python3-samba amd64 2:4.15.13+dfsg-0ubuntu1.6 [3,115 kB]
Get:16 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 samba-common all 2:4.15.13+dfsg-0ubuntu1.6 [75.7 kB]
Get:17 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 samba-common-bin amd64 2:4.15.13+dfsg-0ubuntu1.6 [620 kB]
Get:18 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 tdb-tools amd64 1.4.5-2build1 [26.2 kB]
Get:19 http://ec.archive.ubuntu.com/ubuntu jammy-updates/main amd64 samba amd64 2:4.15.13+dfsg-0ubuntu1.6 [1,192 kB]
Get:20 http://ec.archive.ubuntu.com/ubuntu jammy/main amd64 attr amd64 1:2.5.1-1build1 [22.6 kB]
```

Ilustración 13 - Proceso de instalación de SAMBA

Una vez finalizada la instalación de samba se debe validar que el servicio este funcionado y se esté ejecutando, usando el comando:

systemctl status smbd

```
root@lab4:~# systemctl status smbd
● smbd.service - Samba SMB Daemon
     Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2024-04-12 07:42:49 UTC; 7min ago
       Docs: man:smbd(8)
             man:samba(7)
             man:smb.conf(5)
    Process: 18736 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
   Main PID: 18745 (smbd)
     Status: "smbd: ready to serve connections..."
      Tasks: 4 (limit: 9346)
     Memory: 10.4M
        CPU: 221ms
     CGroup: /system.slice/smbd.service
             ├─18745 /usr/sbin/smbd --foreground --no-process-group
             ├─18747 /usr/sbin/smbd --foreground --no-process-group
             ├─18748 /usr/sbin/smbd --foreground --no-process-group
             └─18749 /usr/lib/x86_64-linux-gnu/samba/samba-bgqd --ready-signal-fd=45 --parent-watch-fd=11 --debuglevel=0 -F

Apr 12 07:42:49 lab4 systemd[1]: Starting Samba SMB Daemon...
Apr 12 07:42:49 lab4 update-apparmor-samba-profile[18739]: grep: /etc/apparmor.d/samba/smbd-shares: No such file or directory
Apr 12 07:42:49 lab4 update-apparmor-samba-profile[18742]: diff: /etc/apparmor.d/samba/smbd-shares: No such file or directory
Apr 12 07:42:49 lab4 systemd[1]: Started Samba SMB Daemon.
root@lab4:~#
root@lab4:~#
root@lab4:~#
```

Ilustración 14 - Validación del servicio de samba

Una vez finalizada la instalación se procede a hacer vulnerable el sistema de archivos. Esto se realiza a través de la configuración del archivo smb.conf.

En este archivo se tiene en cuenta dos puntos importantes de error de configuración:

1. Permitir que cualquiera pueda tener permiso a la ruta compartida sin autenticación.
2. Crear la carpeta en la ruta de los archivos sistemas, esto permitiría que cualquier usuario al tener acceso a la ruta pueda acceder a los archivos del sistema.

Se accede a la ruta del archivo usando vim para editarlo:

vim /etc/samba/smb.conf

```
root@lab4:~# vim /etc/samba/smb.conf
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin



[CarpetaCompartida]
   path = /etc/CarpetaCompartida
   browseable = yes
   writable = yes
   guest ok = yes
   read only = no
   force user = nobody
```

Ilustración 15 - Configuración de la carpeta compartida

Esta configuración crea un recurso compartido sin restricciones, accesible por cualquier usuario, incluso sin autenticación (`guest ok = yes`), lo que representa una vulnerabilidad significativa.

Se reinician los servicios de samba a través del comando:

sudo systemctl restart smbd

```
root@lab4:~#
root@lab4:~# systemctl restart smbd
root@lab4:~#
root@lab4:~#
```

Ilustración 16 - Reinicio de servicio de samba

Se crea la carpeta en la ruta de los archivos del sistema, para ello se utiliza el comando:

mkdir /etc/CarpetaCompartida

```
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida# pwd
/etc/CarpetaCompartida
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida# mkdir /etc/CarpetaCompartida
```

Ilustración 17 - Creación de la carpeta compartida

Se conceden todos los permisos a esta carpeta con el comando:

sudo chmod 777 /etc/CarpetaCompartida/

```
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida# sudo chmod 777 /etc/CarpetaCompartida/
root@lab4:/etc/CarpetaCompartida#
root@lab4:/etc/CarpetaCompartida#
```

Ilustración 18 - Comando de permisos

```
rwxr-xr-x  2 root root        4096 Feb 16 18:51 bash_completion.d
rw-r--r--  1 root root         367 Dec 16  2020 bindresvport.blacklist
rwxr-xr-x  2 root root        4096 Nov 21 20:57 binfmt.d
rwxr-xr-x  2 root root        4096 Feb 16 18:51 byobu
rwxr-xr-x  3 root root        4096 Feb 16 18:44 ca-certificates
rw-r--r--  1 root root        5892 Feb 16 18:45 ca-certificates.conf
rwxrwxrwx  2 root root        4096 Apr 12 08:12 CarpetaCompartida
rwxr-xr-x  5 root root        4096 Apr 12 06:41 cloud
rwxr-xr-x  2 root root        4096 Apr 12 06:39 console-setup
rwxr-xr-x  2 root root        4096 Feb 16 18:50 cron.d
rwxr-xr-x  2 root root        4096 Apr 12 07:42 cron.daily
rwxr-xr-x  2 root root        4096 Feb 16 18:50 cron.hourly
```

Ilustración 19 - Validación de permisos completos

Se valida que las configuraciones estén correctas con el siguiente comando:

sudo testparm

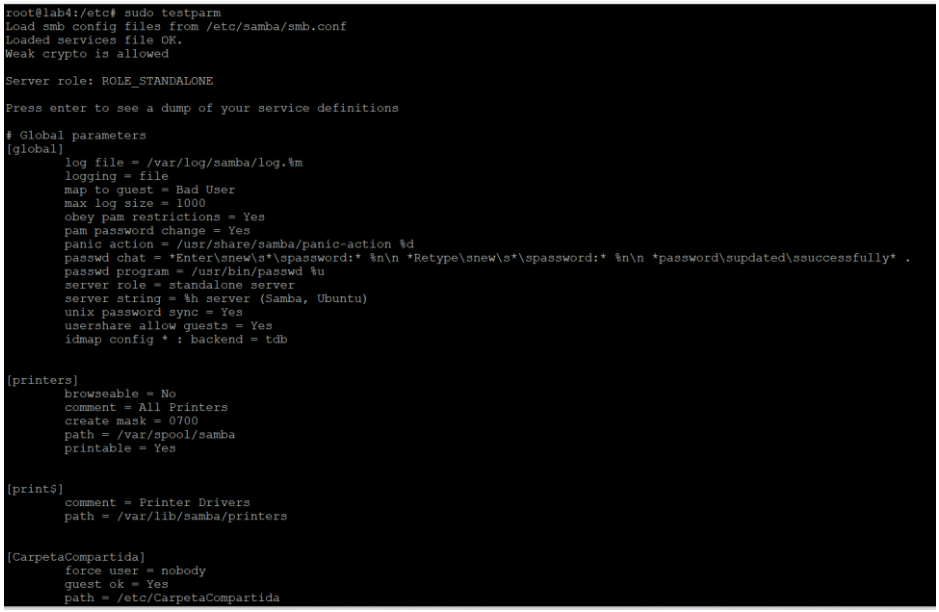


Ilustración 20 - Verificación de recursos compartidos

Con esto se ha finalizado la instalación de samba y sus configuraciones vulnerables.

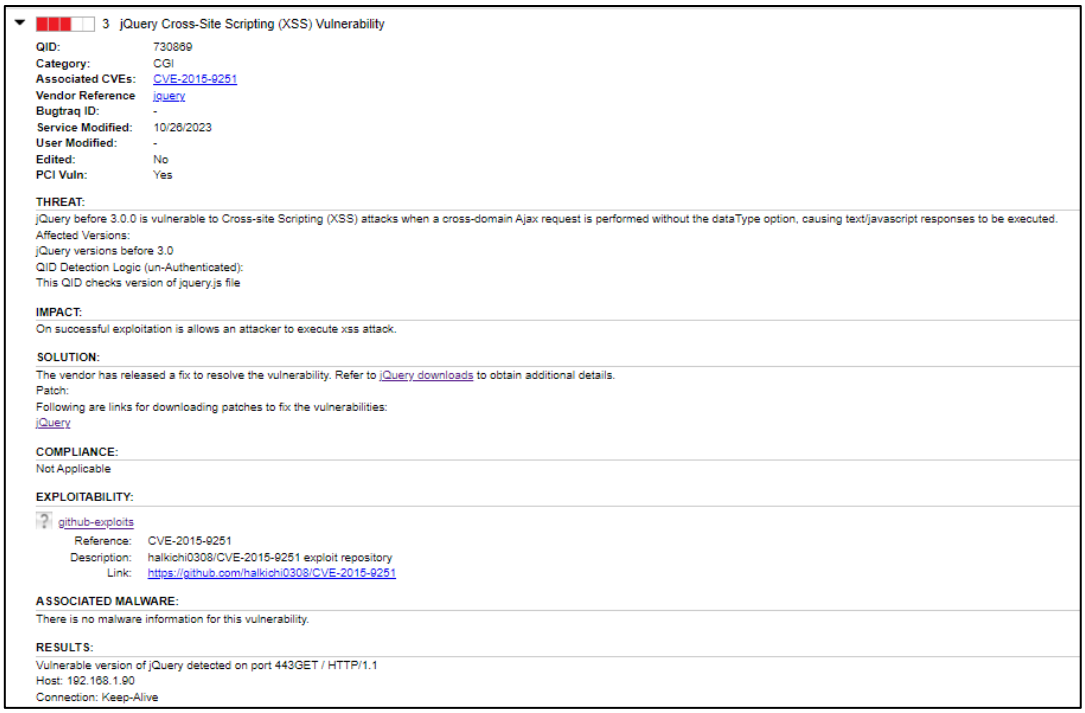
El servidor está listo para la siguiente etapa, la cual es la escaneo y gestión de vulnerabilidades.

Escaneo de vulnerabilidades

Después de la configuración inicial del servidor, se lleva a cabo un escaneo de vulnerabilidades utilizando la herramienta QUALYS, el cual arroja un informe detallado de las siguientes vulnerabilidades identificadas en el servidor.

Vulnerabilidad XSS relacionada con versiones antiguas de jquery

La vulnerabilidad mostrada en la *Ilustración 21* es un problema de Cross-Site Scripting (XSS) asociado con versiones antiguas de jQuery, específicamente antes de la versión 3.0.0. Esta vulnerabilidad permite a un atacante inyectar código JavaScript o HTML malicioso en las páginas vistas por otros usuarios. Esto puede resultar en robo de cookies, secuestro de sesiones y una variedad de ataques contra usuarios de la aplicación web afectada. La vulnerabilidad XSS que se visualiza en la *Ilustración 21* se debe a que se instaló la versión 7.4 de Xamp que incluye la versión 1.10 de jQuery la cual es antigua y es vulnerable a ataques XSS.



3 jQuery Cross-Site Scripting (XSS) Vulnerability

QID: 730869
Category: CGI
Associated CVEs: CVE-2015-9251
Vendor Reference jquery
Bugtraq ID: -
Service Modified: 10/26/2023
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
Affected Versions:
jQuery versions before 3.0
QID Detection Logic (un-Authenticated):
This QID checks version of jquery.js file

IMPACT:
On successful exploitation is allows an attacker to execute xss attack.

SOLUTION:
The vendor has released a fix to resolve the vulnerability. Refer to jQuery downloads to obtain additional details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
jQuery

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
github-exploits
Reference: CVE-2015-9251
Description: halkichi0308/CVE-2015-9251 exploit repository
Link: https://github.com/halkichi0308/CVE-2015-9251

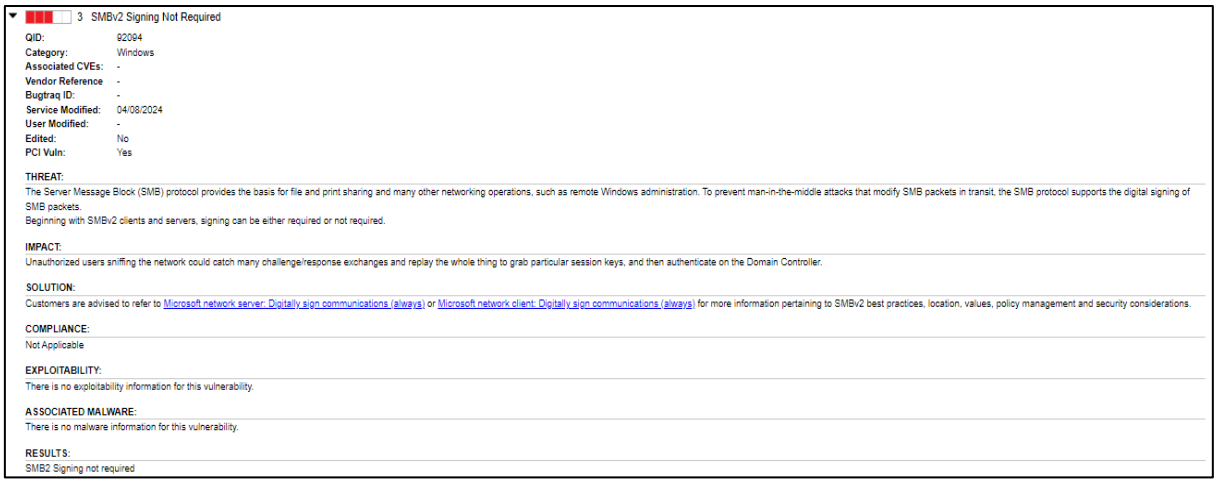
ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable version of jQuery detected on port 443GET / HTTP/1.1
Host: 192.168.1.90
Connection: Keep-Alive

Ilustración 21 - jquery xss vulnerability

Vulnerabilidad SMB

En la Ilustración 22 se observa que el servidor tiene la vulnerabilidad "SMBv2 Signing Not Required" que se refiere a una configuración en la cual el protocolo Server Message Block versión 2 (SMBv2) no requiere la firma de los mensajes. SMB es un protocolo utilizado para compartir archivos, impresoras y otros recursos en una red. La firma de mensajes es una medida de seguridad que asegura que los paquetes SMB no sean interceptados ni alterados durante su transmisión, lo que previene los ataques de "man-in-the-middle" (MitM). Cuando la firma de mensajes SMB no es obligatoria, un atacante que pueda situarse en la red entre dos sistemas que están comunicándose un "man-in-the-middle"podría interceptar y posiblemente modificar los mensajes SMB. Por ejemplo, podrían modificar un paquete de respuesta a una solicitud de autenticación para obtener acceso no autorizado o manipular los datos que se están transmitiendo.



3 SMBv2 Signing Not Required

QID: 92094
Category: Windows
Associated CVEs: -
Vendor Reference -
Bugtraq ID: -
Service Modified: 04/08/2024
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:
The Server Message Block (SMB) protocol provides the basis for file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets.
Beginning with SMBv2 clients and servers, signing can be either required or not required.

IMPACT:
Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:
Customers are advised to refer to Microsoft network server: Digitally sign communications (always) or Microsoft network client: Digitally sign communications (always) for more information pertaining to SMBv2 best practices, location, values, policy management and security considerations.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SMB2 Signing not required

Ilustración 22 - SMBv2 Signing Not Required

Vulnerabilidades en el archivo smb.conf

En la *Ilustración 23* se expone la configuración presente en el archivo smb.conf:

```
[CarpetaCompartida]
        force user = nobody
        guest ok = Yes
        path = /etc/CarpetaCompartida
```

Ilustración 23 - Configuración smb.conf

La configuración realizada presenta varios errores los cuales se detallan a continuación:

Force user = nobody:

Permite a los usuarios acceder a los permisos del usuario "nobody", lo cual dificulta la auditoría de las acciones realizadas por los usuarios, ya que todas las acciones aparecerán bajo el usuario "nobody".

Guest ok = Yes:

Facilita el acceso a las carpetas compartidas sin necesidad de autenticación, lo que posibilita que cualquier persona pueda acceder y modificar el contenido de los archivos sin restricciones.

Path = /etc/CarpetaCompartida:

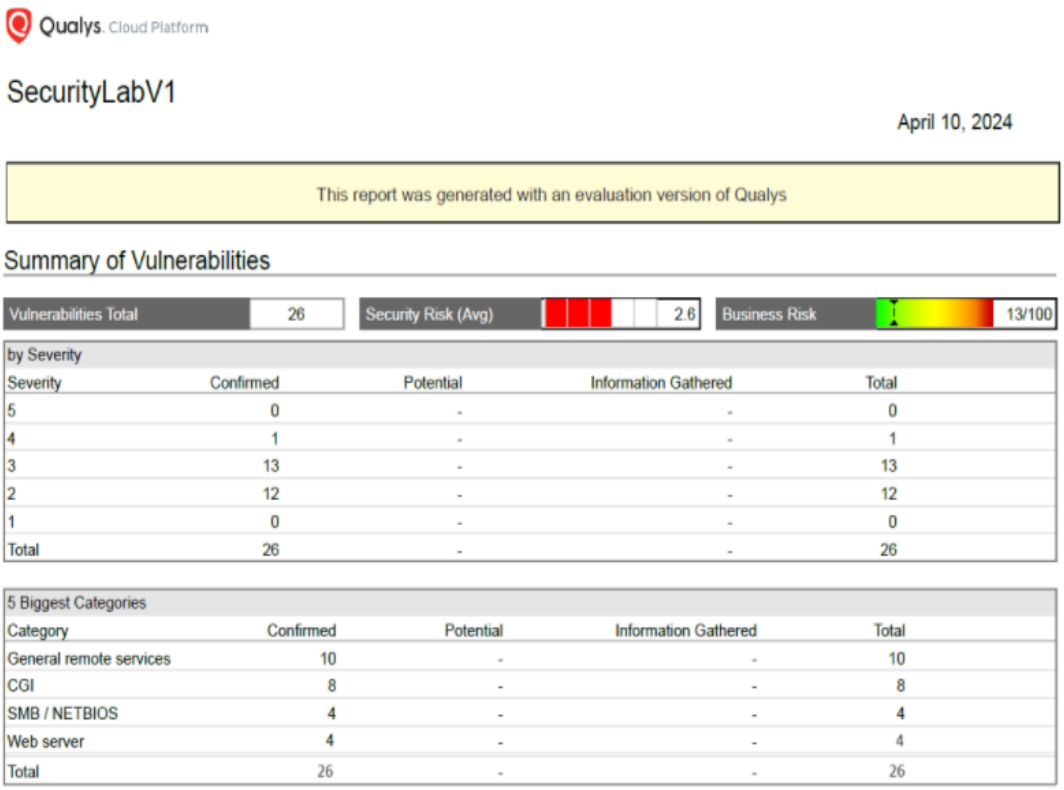
Se comparte una carpeta ubicada en /etc., un directorio estándar para archivos de configuración en sistemas Linux. Compartir aquí es arriesgado, ya que podría permitir a un atacante modificar configuraciones del sistema si se le dan permisos de escritura.

Read only = No:

Esta configuración habilita la escritura en la carpeta compartida. Al combinarla con el acceso de invitado (guest ok), implica que cualquier individuo en la red no solo puede leer, sino también escribir y borrar archivos en esta carpeta.

Análisis de vulnerabilidades

Se utiliza Qualys para llevar a cabo el análisis de vulnerabilidades, una herramienta diseñada para la gestión y detección de dichas vulnerabilidades. A través de esta herramienta, generamos el *Reporte_Vulnerabilidades_V1*, el cual detalla la cantidad de vulnerabilidades presentes en el servidor. En este informe, identificamos un total de 26 vulnerabilidades distribuidas en 4 categorías: servicios remotos, CGI, SMB y servidor web.



Qualys. Cloud Platform

SecurityLabV1

April 10, 2024

This report was generated with an evaluation version of Qualys

Summary of Vulnerabilities

Vulnerabilities Total	26	Security Risk (Avg)	2.6	Business Risk	13/100

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	1	-	-	1
3	13	-	-	13
2	12	-	-	12
1	0	-	-	0
Total	26	-	-	26

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	10	-	-	10
CGI	8	-	-	8
SMB / NETBIOS	4	-	-	4
Web server	4	-	-	4
Total	26	-	-	26

Ilustración 24 – Vulnerabilidades

En la *Ilustración 25* se presenta la gravedad de las 26 vulnerabilidades detectadas según la clasificación de Qualys, donde se asigna un nivel del 1 al 5, siendo 1 el menos grave y 5 el más grave.

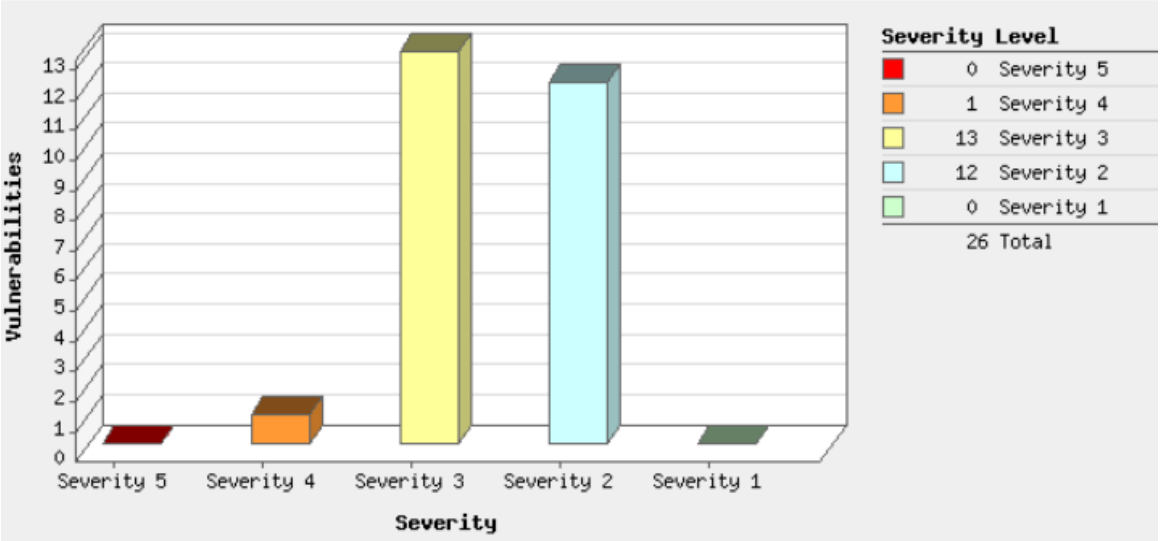


Ilustración 25 - Severidad de las vulnerabilidades

Una vez realizado el escaneo de vulnerabilidades, se procede a corregirlas mediante los siguientes procedimientos:

1. Reinstalación de Ubuntu con parches
2. Gestionar la vulnerabilidad XSS

Para gestionar la vulnerabilidad XSS relacionada con versiones antiguas de jquery, llevar a cabo las siguientes actividades:

Actualizar jQuery:

Actualizar la biblioteca jQuery a la versión más reciente que aborde esta vulnerabilidad es prioritario. Se recomienda utilizar cualquier versión posterior a la 3.0.0. En caso de no ser posible, aplicar los parches disponibles.

Revisar el Código:

Es fundamental auditar todas las solicitudes Ajax en el código fuente de la aplicación para garantizar un manejo adecuado de las respuestas y establecer el tipo de datos esperado (dataType). Esto ayudará a prevenir la ejecución involuntaria de scripts no deseados.

Validación y Sanitización:

Es importante validar y sanear todas las entradas del usuario, tanto en el lado del cliente como en el del servidor, con el fin de evitar posibles inyecciones maliciosas.

Corrección de Configuraciones:

Configurar adecuadamente el servidor y los encabezados HTTP para restringir las peticiones de dominio cruzado solo a dominios de confianza.

Pruebas y Validación:

Realizar pruebas de penetración después de aplicar los cambios para confirmar que la vulnerabilidad ha sido efectivamente mitigada.

3. Gestionar la vulnerabilidad SMB

Para abordar las vulnerabilidades relacionadas con la configuración de Samba, es crucial realizar ajustes en la configuración para asegurar la carpeta compartida. Esto implica seguir una serie de pasos recomendados, los cuales se detallan con mayor precisión en el anexo "Informe de Mitigación de Vulnerabilidades".

- Modificar el parámetro **guest ok = Yes** a **guest ok = No**. Esta acción exigirá que todos los usuarios se autentiquen antes de poder acceder a la carpeta compartida.
- Eliminar o comentar la línea ***force user = nobody***. En su lugar, configurar Samba para que utilice cuentas de usuario válidas que tengan permisos restringidos sobre los archivos que se comparten, asignar usuarios específicos y restringir el acceso solo a esos usuarios.
- Cambiar la ubicación de la carpeta compartida fuera del directorio `/etc`, ya que no es una práctica segura compartir una carpeta de configuración del sistema.
- Configurar el parámetro read only = Yes para prevenir la modificación de archivos, garantizando así su integridad.
- Usar los comandos `chown` y `chmod` para asegurar que los archivos y directorios dentro de la carpeta compartida tengan los propietarios y permisos adecuados.
- Implementar listas de control de acceso de red para restringir qué direcciones IP pueden acceder a la carpeta compartida.
- Configurar Samba para registrar quién accede a la carpeta y qué operaciones se realizan.

- Verificar que se ejecute la última versión de Samba con todas las actualizaciones de seguridad aplicadas.
- Configurar Samba para usar SMB3 con encriptación.

5. Resultados y discusión

Después de aplicar las medidas de mitigación detalladas y adoptar buenas prácticas de seguridad en respuesta al análisis de vulnerabilidades del informe "Reporte_Vulnerabilidades_V1.pdf", hemos notado una mejora significativa en la seguridad del entorno del servidor WebServer/FileServer. Esto se refleja en la *Ilustración 26*, donde se observa que el número de vulnerabilidades detectadas ha disminuido a solo 6, cubriendo únicamente 3 categorías: SMB, TCP y servicios remotos. Para obtener más detalles sobre este progreso, se puede consultar el anexo "Reporte_Vulnerabilidades_V2.pdf".

Summary of Vulnerabilities

Vulnerabilities Total	6	Security Risk (Avg)	2.7	Business Risk	13/100

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	4	-	-	4
2	2	-	-	2
1	0	-	-	0
Total	6	-	-	6

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
SMB / NETBIOS	4	-	-	4
TCP/IP	1	-	-	1
General remote services	1	-	-	1
Total	6	-	-	6

Ilustración 26 - Escaneo final de vulnerabilidades

Las acciones adoptadas han abordado de manera efectiva las vulnerabilidades críticas identificadas, particularmente aquellas relacionadas con los servicios SMBv2, el servidor Apache HTTP y la biblioteca jQuery. Además, se han realizado actualizaciones pertinentes en componentes clave del sistema, tales como PHP y MySQL, a versiones más seguras, y se ha llevado a cabo una configuración meticulosa de los parámetros de seguridad para Apache2.

La actualización de Apache y la eliminación de versiones obsoletas y vulnerables del software aseguran que el servidor está protegido contra explotaciones conocidas que podrían comprometer la integridad y disponibilidad de los servicios web. La implementación de una configuración segura.

Las vulnerabilidades visualizadas en la Ilustración 26 y en el documento "Reporte_Vulnerabilidades_V2.pdf" se han identificado como falsos positivos. Por lo tanto, se ha optado por aceptar el riesgo asociado a través del Documento de Aceptación del Riesgo, el cual estará disponible en los anexos.

Este enfoque proactivo y exhaustivo ha fortalecido significativamente la infraestructura de seguridad del entorno del servidor, reduciendo de manera notable las posibles vulnerabilidades y estableciendo una base sólida para la protección continua contra amenazas futuras.

6. Conclusiones

La configuración inadecuada de servidores web y archivos compartidos representa una seria amenaza para la seguridad de la información, pudiendo desencadenar incidentes catastróficos y la pérdida de datos sensibles ante la actividad maliciosa de ciberdelincuentes. Aspectos como la falta de actualización de sistemas operativos, la exposición de puertos y servicios a explotaciones, así como las vulnerabilidades en aplicaciones web, aumentan significativamente el riesgo de compromiso de la integridad y confidencialidad de los datos.

Para obtener los resultados previstos en el proyecto, fue necesario deliberadamente configurar los servidores de manera incorrecta. Esto incluyó desde no aplicar parches de seguridad actualizados hasta exponer credenciales sensibles, así como dejar puertos abiertos, lo que resultó en una vulnerabilidad de seguridad. Esta estrategia nos permitió identificar y analizar minuciosamente las vulnerabilidades en los servidores web, servidores de archivos compartidos, así como en las áreas de XSS y gestión de permisos.

Con lo mencionado anteriormente, se logra identificar la vulnerabilidad en XSS asociada con versiones obsoletas de jquery. De la misma forma, se evidencia la vulnerabilidad en SMB cuando la firma de mensajes no es obligatoria. En tales casos, un atacante situado en la red entre dos sistemas comunicándose podría realizar un ataque "man-in-the-middle", interceptando y posiblemente modificando los mensajes SMB. Además, se enfoca en hacer que las carpetas compartidas sean un objetivo para su vulneración otorgando permisos de control total.

En este sentido, se concluye que es crucial implementar configuraciones seguras en los servidores, priorizando la actualización de sistemas operativos a sus últimas versiones para mitigar las vulnerabilidades asociadas a la obsolescencia. Especial atención debe darse a la configuración adecuada de herramientas como Samba, evitando la exposición de puertos críticos como los 137, 138 y 445, los cuales podrían ser explotados para comprometer toda la red. Además, es fundamental mantener actualizados los aplicativos, como XAMPP, con el fin de prevenir vulnerabilidades como las de tipo XSS.

Se subraya la importancia de considerar la seguridad como un aspecto primordial en todas las fases del desarrollo y la gestión de sistemas, reconociendo que un

conocimiento profundo de las vulnerabilidades y las técnicas de ataque es esencial para diseñar sistemas y aplicaciones resilientes ante las amenazas cibernéticas. Por último, se recalca la responsabilidad ética de utilizar dicho conocimiento para fortalecer la seguridad de manera proactiva, en lugar de aprovecharse de las debilidades con fines maliciosos.

7. Referencias

[1] L. J. Aguilar, Computación en la nube, Alpha Editorial, 2012.

[2] V. E. y. G. Julio, «Virtualización de servidores de telefonía IP en GNU/LINUX,» [En línea]. Available: http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf. [Último acceso: 16 noviembre 2023].

[3] M. D. G. Río, Tecnologías de Virtualización, CreateSpace Independent Publishing Platform, 2014.

[4] N. S. C. JIMENEZ, «HACKING WEB (ANÁLISIS DE ATAQUES SQL Inyección, XSS),» Cartagena , 2019.

[5] «FASTERCAPITAL,» 07 12 2023. [En línea]. Available: https://fastercapital.com/es/contenido/Permisos-de-usuario--Gestion-de-permisos-de-usuario-en-la-autorizacion-Configuracion-solo.html. [Último acceso: 04 01 2024].

[6] J. C. G. RICO, «Así enfrenta Colombia su primer caso de 'megasecuestro digital'; ¿qué está pasando?,» *El tiempo ,* 18 septiembre 2023.

[7] D. J. M. TIPAN, «Análisis de herramientas de virtualización como soporte al modelo de negocio de las PYMES,» Babahoyo , 2023.

[8] M. R. I. R. A. A. S. G. F. N. Sultan Abdullah Algarni, «Evaluación de rendimiento de hipervisores Xen, KVM y Proxmox,» *International Journal of Open Source Software and Processes (IJOSSP),* p. 16, 2018.

[9] R. R. A. Rudibel Perdigón Llanes, «Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas,» *Revista Cubana de Ciencias Informáticas,* vol. 14, nº 1, p. 17, 2020.

[10] G. Fernández Fernández, «Elementos de sistemas operativos, de representación de la información y de procesadores hardware y software,» ARCHIVO DIGITAL UPM, Madrid, 2015.

[11] A. N. R. C. W. L. Loor Cevallos, «"Desarrollo de un aplicativo web para el agendamiento de citas médicas dirigido al "Patronato de Amparo Social" del cantón La Maná".,» 08 2023.

[En línea]. Available: http://repositorio.utc.edu.ec/handle/27000/11320. [Último acceso: 20 11 2023].

[12] K. P. P. Guashpa, «MANUAL DE IMPLEMENTACIÓN DE UN PROCESO HARDENING PARA MITIGAR VULNERABILIDADES EN EL SERVIDOR WEB NGINX DE LA UNACH,» *UNIVERSIDAD NACIONAL DE CHIMBORAZO,* p. 68, 2022.

[13] L. G. Marquina Fernández, «Repositorio Institucional de la UTP,» 2020. [En línea]. Available: https://repositorio.utp.edu.pe/handle/20.500.12867/3776. [Último acceso: 20 11 2023].

[14] J. A. Castro, «Herramienta PROXMOX como plataforma tecnológica para la virtualización de servidores en la organización.,» *Revista Aula Virtual,* vol. 4, nº 9, p. 12, 2023.

[15] S. Wibowo, «Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd,» *Indonesian Journal of Information Systems,* vol. 3, nº 2, p. 10, 2021.

[16] A. A. d. Cárdenas, «Auditoría Técnica de seguridad: análisis y explotación de vulnerabilidades,» Madrid, 2018.

[17] D. F. N. VASQUEZ, «DISEÑO DE UN MODELO DE VIRTUALIZACIÓN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SERVIDORES EN ALTA DISPONIBILIDAD,» Bogotá , 2020.

[18] C. L. G. V. A. E. A. E. MARÍA BELÉN SOTAMINGA REYES, «Implementación de un ambiente de Virtualización para el manejo de múltiples servidores de VoIP sobre una plataforma común de hardware,» GUAYAQUIL, 2011.

[19] J. E. M. Medrano, «Análisis de Seguridad Web para Prevenir Cross-Site Scripting (XSS) en Aplicaciones PHP,» CIMAT Zacatecas, Zacatecas , 2011.

[20] W. A. P. C. Brayan David Carrasco Cabezas, Diseño de una infraestructura de escritorios virtuales, utilizando tecnología VMware y Uds Enterprise para la publicación de servicios VDI sobre Moodle.t, Riobamba , 2022.

[21] B. F. M. A. Villa Camargo María Rocío, «Implementación de remediaciones de vulnerabilidades identificadas en aplicaciones desarrolladas en PHP (V 7.4.33) sobre un servidor con sistema operativo Linux (Ubuntu), mediante escaneos de seguridad (OWASP) realizados en una empresa pyme de Call Center,» Corporación Universitaria Unitec, Bogotá , 2023.

[22] Ubuntu, «Ubuntu,» 2011 10 18. [En línea]. Available: https://www.guia-ubuntu.com/index.php/Ubuntu. [Último acceso: 10 04 2024].

[23] R. C. Bou, Usando XAMPP con Bootstrap y WordPress, Rama Solutions, 2019.

[24] D. M. G. Pablo Martínez Pérez, «El protocolo de compartición de recursos en red SMB y sus recientes vulnerabilidades,» *Revista de la Escuela de Ingeniería Informática de Segovi,* nº 05, p. 9, 2017.

[25] J. J. D. J. J. R. G. H. A. Michael Stiven Lopez Amaya, «CONSULTORÍA DE SEGURIDAD PARA EL ANÁLISIS Y REMEDIACIÓN DE VULNERABILIDADES,» Bogotá, 2023.

8. Anexos

Anexo 1: Reporte_Vulnerabilidades_V1

En el Anexo 1 se puede visualizar el reporte generado con la herramienta Qualys como se muestra en la Ilustración 27 tenemos el conocimiento del total de vulnerabilidades encontradas, el nivel de riesgo y cuáles son los servicios que se encuentras afectados.

Qualys. Cloud Platform

SecurityLabV1

April 10, 2024

This report was generated with an evaluation version of Qualys

Report Summary

User Name:	Usuario1
Login Name:	techn3rc1
Company:	-
User Role:	Manager
Address:	samanes
Zip:	090502
Country:	Ecuador
Created:	04/10/2024 at 10:32:15 AM (GMT+0000)
Template Title:	Technical Report
Asset Groups:	SecurityLab
IPs:	-
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 04/10/2024
Active Hosts:	2
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	26	Security Risk (Avg)	2.6	Business Risk	13/100

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	1	-	-	1
3	13	-	-	13
2	12	-	-	12
1	0	-	-	0
Total	26	-	-	26

5 Biggest Categories

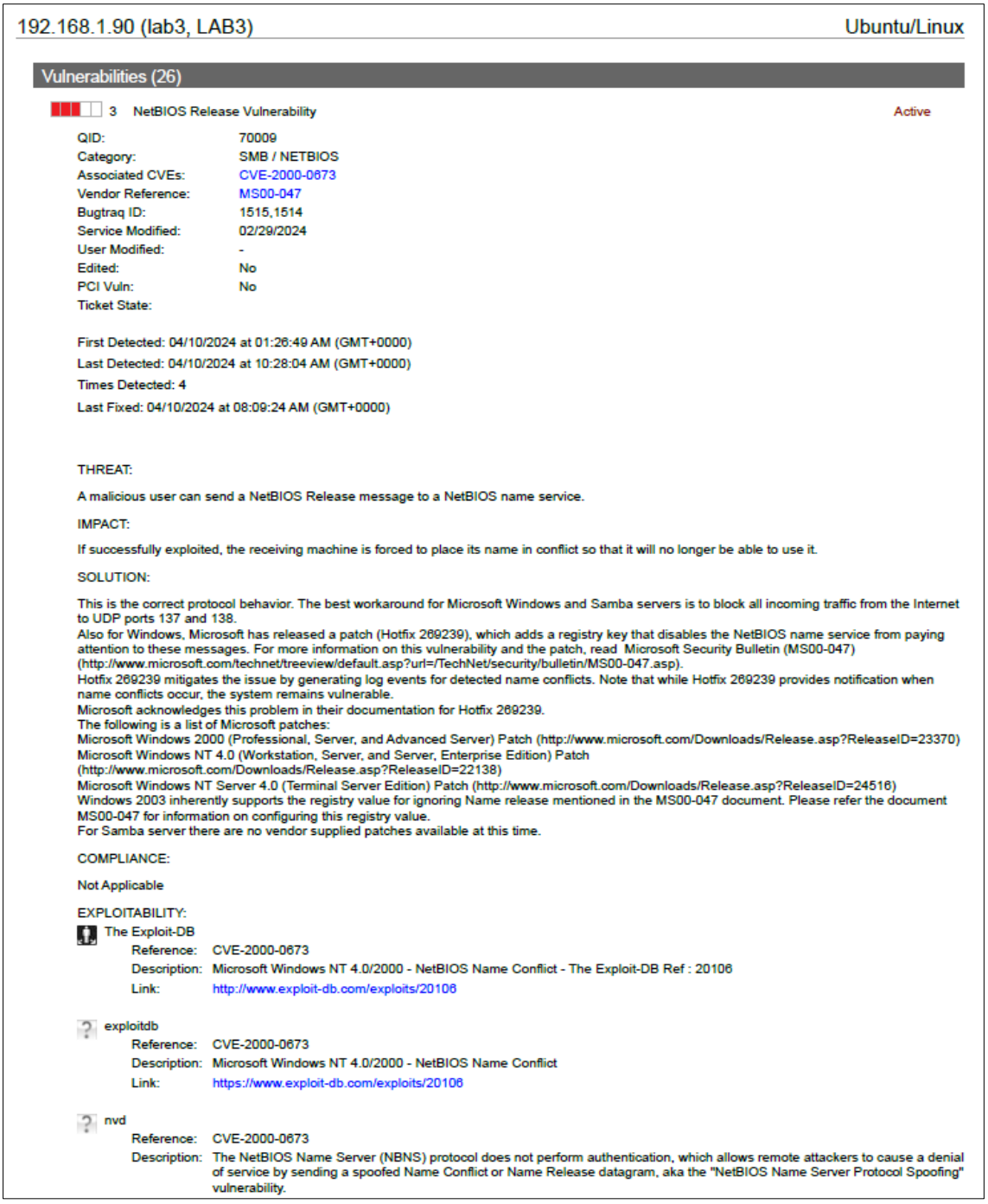
Category	Confirmed	Potential	Information Gathered	Total
General remote services	10	-	-	10
CGI	8	-	-	8
SMB / NETBIOS	4	-	-	4
Web server	4	-	-	4
Total	26	-	-	26

Ilustración 27 Resumen del reporte de vulnerabilidades

La Ilustración 28 ofrece un diagrama de barras que detalla el nivel de riesgo asociado con cada vulnerabilidad identificada. Este gráfico proporciona una representación visual clara y concisa de la gravedad de las vulnerabilidades, permitiendo una evaluación más precisa de las posibles amenazas. Además, ayuda a priorizar las medidas de mitigación y asignar recursos adecuadamente para abordar las áreas de mayor riesgo, facilitando así a los responsables de seguridad y a los tomadores de decisiones comprender dónde concentrar los esfuerzos para mejorar la seguridad del sistema.

Ilustración 28 Diagrama de barras con niveles de vulnerabilidad

Mediante el empleo de QUALYS, se realizó un escaneo minucioso que abarcó diversas vulnerabilidades, entre las cuales se incluyó la referente a SMB, como se evidencia en la Ilustración 29, donde se identificó un nivel de riesgo 3. Esta herramienta proporcionó un análisis exhaustivo, permitiendo no solo la detección de las vulnerabilidades, sino también la evaluación precisa de su posible impacto en el sistema. Además, ofreció recomendaciones concretas para abordar cada vulnerabilidad, facilitando así la implementación de soluciones efectivas y la mejora de la seguridad del sistema en general.



192.168.1.90 (lab3, LAB3) Ubuntu/Linux

Vulnerabilities (26)

3 NetBIOS Release Vulnerability Active

QID:	70009
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1515,1514
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 4
Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

A malicious user can send a NetBIOS Release message to a NetBIOS name service.

IMPACT:

If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.

SOLUTION:

This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and 138.
Also for Windows, Microsoft has released a patch (Hotfix 269239), which adds a registry key that disables the NetBIOS name service from paying attention to these messages. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable.
Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows 2000 (Professional, Server, and Advanced Server) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23370)
Microsoft Windows NT 4.0 (Workstation, Server, and Server, Enterprise Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22138)
Microsoft Windows NT Server 4.0 (Terminal Server Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24516)
Windows 2003 inherently supports the registry value for ignoring Name release mentioned in the MS00-047 document. Please refer the document MS00-047 for information on configuring this registry value.
For Samba server there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link: http://www.exploit-db.com/exploits/20106

exploitdb
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict
Link: https://www.exploit-db.com/exploits/20106

nvd
Reference: CVE-2000-0673
Description: The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.

Ilustración 29 Informe de escaneo SMB

Observando la Ilustración 30 y analizando el informe proporcionado por QUALYS, podemos concluir que SMBv2 facilita diversas funciones de red, como el intercambio de archivos, la impresión y la administración remota de Windows. A pesar de que el protocolo SMB incorpora medidas de seguridad, como la firma digital para autenticar los mensajes, en este caso se registró un nivel de riesgo 3. Esto implica que los atacantes que monitorean la red podrían interceptar y reproducir numerosos intercambios de desafío y respuesta, potencialmente obteniendo acceso a claves de sesión específicas.

Link: http://www.securityfocus.com/bid/1514

seebug
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4/2000 NetBIOS Name Conflict Vulnerability
Link: https://www.seebug.org/vuldb/ssvid-74002

nist-nvd2
Reference: CVE-2000-0673
Description: The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.
Link: http://www.securityfocus.com/bid/1514

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

3 SMBv2 Signing Not Required Active

QID: 92094
Category: Windows
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/08/2024
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 4
Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

The Server Message Block (SMB) protocol provides the basis for file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets.
Beginning with SMBv2 clients and servers, signing can be either required or not required.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Customers are advised to refer to Microsoft network server: Digitally sign communications (always)
(https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always#default-values)
or Microsoft network client: Digitally sign communications (always)
(https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always)
for more information pertaining to SMBv2 best practices, location, values, policy management and security considerations.

COMPLIANCE:

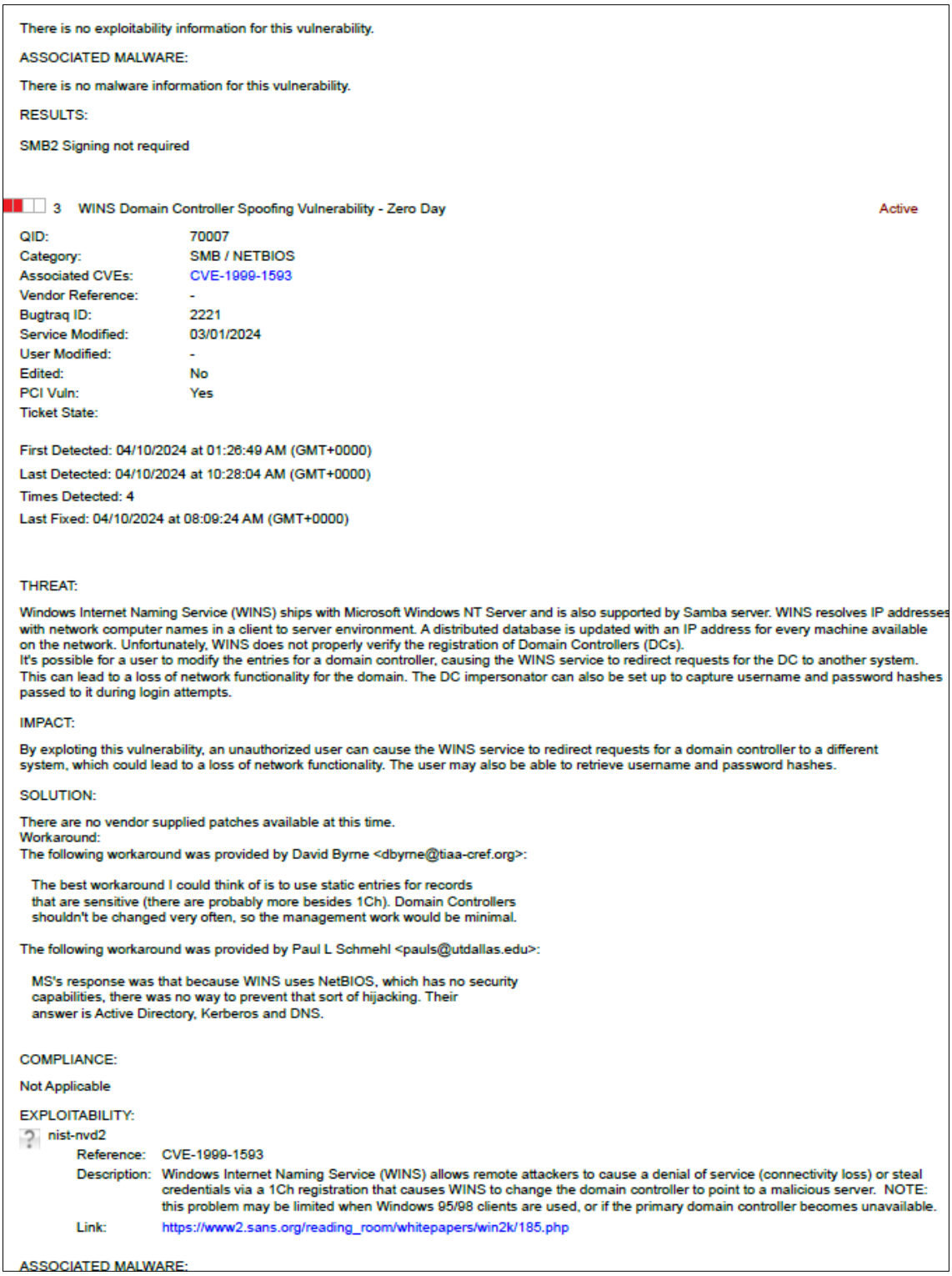
Not Applicable

EXPLOITABILITY:

Ilustración 30 Informe vulnerabilidad SMBv2

El informe revela una vulnerabilidad en SMB/NETBIOS con CVE-1999-1593, donde los atacantes remotos pueden explotar el Servicio de Nombres de Internet de Windows (WINS) para desencadenar una negación de servicio o para robar credenciales. Esto se logra mediante la manipulación de un registro específico que induce a WINS a redirigir las solicitudes del controlador de dominio hacia un servidor malicioso. Es relevante subrayar que este problema puede ser atenuado si se utilizan clientes Windows 95/98 o si el controlador de dominio principal se vuelve inaccesible. Esta situación genera un

impacto significativo, ya que un atacante no autorizado podría dirigir las solicitudes del controlador de dominio hacia otro sistema, potencialmente causando interrupciones en la funcionalidad de la red. Además, el intruso podría obtener hashes de nombre de usuario y contraseña, comprometiendo aún más la seguridad del sistema.



There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SMB2 Signing not required

3 WINS Domain Controller Spoofing Vulnerability - Zero Day Active

QID:	70007
Category:	SMB / NETBIOS
Associated CVEs:	CVE-1999-1593
Vendor Reference:	-
Bugtraq ID:	2221
Service Modified:	03/01/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)

Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)

Times Detected: 4

Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server and is also supported by Samba server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network. Unfortunately, WINS does not properly verify the registration of Domain Controllers (DCs).
It's possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.

IMPACT:

By exploting this vulnerability, an unauthorized user can cause the WINS service to redirect requests for a domain controller to a different system, which could lead to a loss of network functionality. The user may also be able to retrieve username and password hashes.

SOLUTION:

There are no vendor supplied patches available at this time.
Workaround:
The following workaround was provided by David Byrne <dbyrne@tiaa-cref.org>:

The best workaround I could think of is to use static entries for records
that are sensitive (there are probably more besides 1Ch). Domain Controllers
shouldn't be changed very often, so the management work would be minimal.

The following workaround was provided by Paul L Schmehl <pauls@utdallas.edu>:

MS's response was that because WINS uses NetBIOS, which has no security
capabilities, there was no way to prevent that sort of hijacking. Their
answer is Active Directory, Kerberos and DNS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

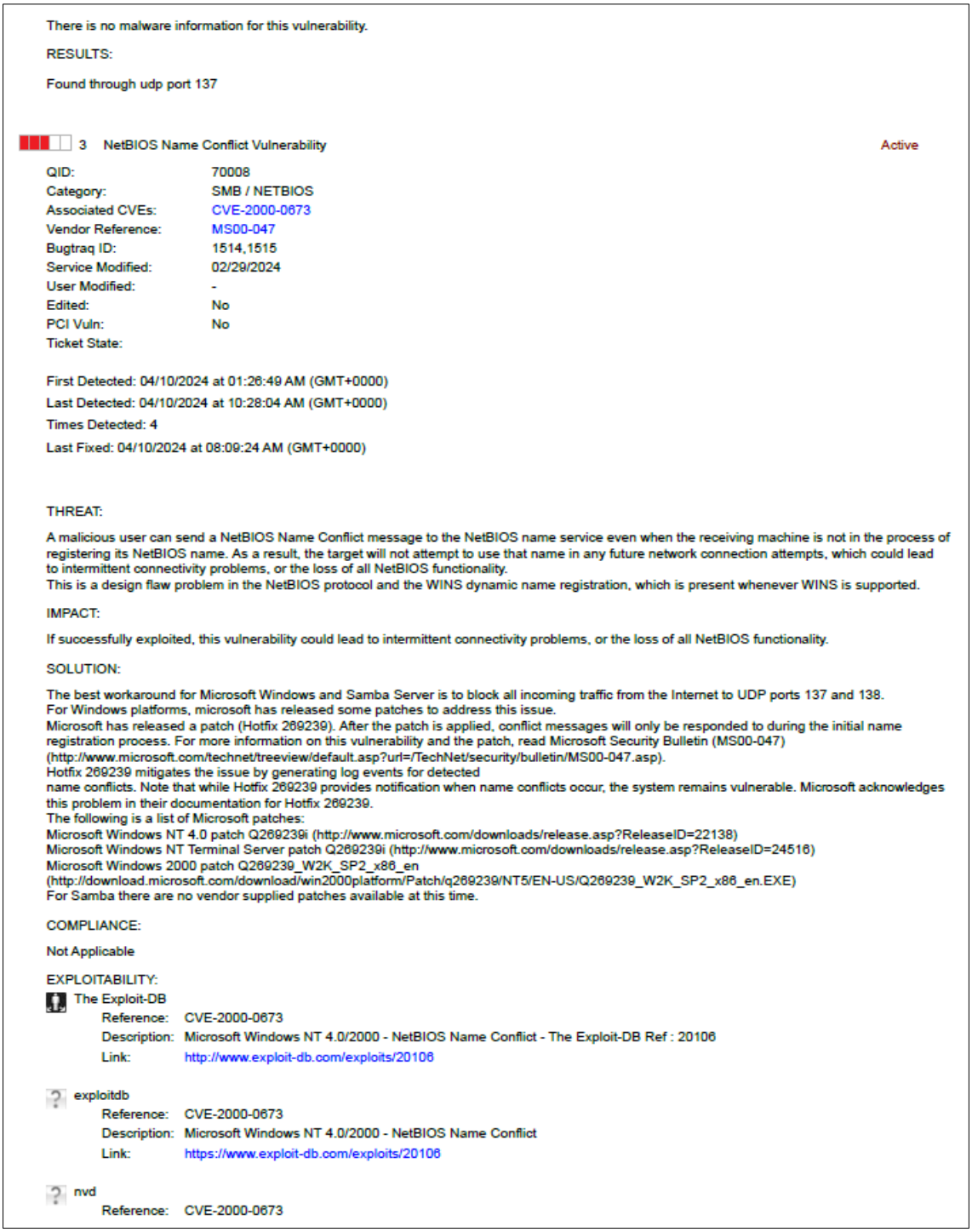
nist-nvd2

Reference:	CVE-1999-1593
Description:	Windows Internet Naming Service (WINS) allows remote attackers to cause a denial of service (connectivity loss) or steal credentials via a 1Ch registration that causes WINS to change the domain controller to point to a malicious server. NOTE: this problem may be limited when Windows 95/98 clients are used, or if the primary domain controller becomes unavailable.
Link:	https://www2.sans.org/reading_room/whitepapers/win2k/185.php

ASSOCIATED MALWARE:

Ilustración 31 Escaneo de WINS Domain Controller Spoofing Vulerability - Zero Day

De acuerdo con la Ilustración 32 el informe indica que este problema surge de una deficiencia de diseño en el protocolo NetBIOS y el registro dinámico de nombres WINS, y se manifiesta cada vez que se habilita el soporte de WINS. Es importante resaltar que esta vulnerabilidad está arraigada en la estructura misma del protocolo, lo que significa que persistirá mientras WINS siga siendo utilizado.



There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

3 NetBIOS Name Conflict Vulnerability — Active

QID:	70008
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1514,1515
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 4
Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, the target will not attempt to use that name in any future network connection attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.
This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.

IMPACT:

If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

SOLUTION:

The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.
For Windows platforms, microsoft has released some patches to address this issue.
Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows NT 4.0 patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=22138)
Microsoft Windows NT Terminal Server patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=24516)
Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en (http://download.microsoft.com/download/win2000platform/Patch/q269239/NT5/EN-US/Q269239_W2K_SP2_x86_en.EXE)
For Samba there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link: http://www.exploit-db.com/exploits/20106

exploitdb
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict
Link: https://www.exploit-db.com/exploits/20106

nvd
Reference: CVE-2000-0673

Ilustración 32 NetBIOS Name Conflict Vulnerability

Dentro del informe, la Ilustración 33 señala que el protocolo SSH (Secure Shell) es una herramienta para establecer conexiones remotas seguras entre computadoras. Sin embargo, se

advierte que este protocolo utiliza configuraciones criptográficas desactualizadas basadas en SHA1, que ha sido desaconsejado. Estas configuraciones presentan vulnerabilidades a los ataques de colisión, los cuales buscan generar el mismo valor hash para distintos conjuntos de datos de entrada. Aunque se asume que cada hash es único, esta vulnerabilidad compromete esta premisa.

2 SHA1 deprecated setting for SSH port 22/tcp Active

QID:	38909
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/06/2023
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 04/09/2024 at 11:35:09 PM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 6
Last Fixed: N/A

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The target is using deprecated SHA1
cryptographic settings to communicate.

IMPACT:

vulnerable to collision attacks, which are designed to fabricate the same hash value for different input data.each hash is supposedly unique.

SOLUTION:

Avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to NIST Retires SHA-1 Cryptographic Algorithm (SSH)
(https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm) .
Other documents to refer
Deprecate settings listed for red hat
(https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.4_release_notes/chap-red_hat_enterprise_linux-7.4_release_notes-deprecated_functionality_in_rhel7)
Key exchange (https://www.ietf.org/archive/id/draft-ietf-curdle-ssh-kex-sha2-13.html)
CBC Cipher (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5161)
Settings currently considered deprecated:
1.Key exchange algorithms:
diffie-hellman-group1-sha1, rsa1024sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, gss-gex-sha1-*, gss-group1-sha1-* and gss-group14-sha1-*.
2.MAC:
hmac-sha1, hmac-sha1-96, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com
3.Host key:
ssh-rsa, ssh-dss, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Type	Name
MAC	hmac-sha1-etm@openssh.com
MAC	hmac-sha1

Ilustración 33 SHA1 deprecated setting for SSH

Los individuos no autorizados pueden acceder al nombre del servidor NetBIOS de este host desde una ubicación remota. Esto plantea un riesgo de seguridad significativo, ya que divulga información confidencial sobre la infraestructura de red del sistema como se puede evidenciar en la Ilustración 34 de acuerdo al informe generado por QUALYS.

Description: The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.

Link: http://www.securityfocus.com/bid/1514

seebug

Reference: CVE-2000-0673

Description: Microsoft Windows NT 4/2000 NetBIOS Name Conflict Vulnerability

Link: https://www.seebug.org/vuldb/ssvid-74002

nist-nvd2

Reference: CVE-2000-0673

Description: The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.

Link: http://www.securityfocus.com/bid/1514

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

2 NetBIOS Name Accessible Active

QID:	70000
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)

Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)

Times Detected: 4

Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:

If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Ilustración 34 NetBIOS Name Accessible

De acuerdo con el CVE-2023-38709 la ausencia de una adecuada validación de entrada en el núcleo de Apache posibilita que generadores de contenido o backend maliciosos o vulnerables fragmenten las respuestas HTTP. Esta vulnerabilidad impacta a los servidores HTTP Apache hasta la versión 2.4.58. Este fallo en la validación de entrada puede ser aprovechado por actores malintencionados para manipular las respuestas HTTP, lo que potencialmente abre la puerta a diversas formas de ataques y explotación como se muestra en la Ilustración 35 así mismo con el CVE-2024-24795 La fragmentación de la respuesta HTTP en diversos módulos del servidor

HTTP Apache posibilita que un atacante pueda introducir encabezados de respuesta maliciosos en las aplicaciones backend, desencadenando así un ataque de desincronización HTTP. Se aconseja a los usuarios que actualicen a la versión 2.4.59 del servidor Apache, ya que esta versión aborda y soluciona este problema de seguridad. Esta actualización es crucial para mitigar el riesgo de explotación de la vulnerabilidad y garantizar la seguridad del servidor como se muestra en la Ilustración 36 de acuerdo con los resultados obtenidos.

3 Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Security Vulnerabilities (CVE-2023-38709, CVE-2024-24795, CVE-2024-27316) — port 443/tcp over SSL — Re-Opened

QID:	731355
Category:	CGI
Associated CVEs:	CVE-2023-38709, CVE-2024-24795, CVE-2024-27316
Vendor Reference:	Apache_http_server
Bugtraq ID:	-
Service Modified:	04/08/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 04/09/2024 at 11:35:09 PM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 4
Last Fixed: 04/10/2024 at 08:49:52 AM (GMT+0000)

THREAT:

Apache HTTP Server is an HTTP web server application.
CVE-2023-38709: Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.
CVE-2024-24795: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.
CVE-2024-27316: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
Affected Versions:
Apache HTTP Server versions prior to 2.4.59

IMPACT:

Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:

Customers are advised to update the latest Apache versions respectively.

Ilustración 35 HTTP Server

For more information, visit here (https://httpd.apache.org/security/vulnerabilities_24.html).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache HTTP Server (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable Apache HTTP Server detected on port 443 -
Date: Wed, 10 Apr 2024 09:15:23 GMT
Server: Apache/2.4.54 (Unix) OpenSSL/1.1.1s PHP/7.4.33 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/7.4.33
Location: https:///dashboard/
Content-Length: 111
Connection: close
Content-Type: text/html; charset=UTF-8

Notice: Undefined index: HTTP_HOST in /opt/lampp/htdocs/index.php on line 7

Ilustración 36 Resultado escaneo de vulnerabilidades

Anexo 2: Reporte_Vulnerabilidades_V2

Qualys. Cloud Platform

SecurityLabV2

April 10, 2024

This report was generated with an evaluation version of Qualys

Report Summary

User Name:	Usuario1
Login Name:	techn3rc1
Company:	-
User Role:	Manager
Address:	samanes
Zip:	090502
Country:	Ecuador
Created:	04/10/2024 at 12:08:49 PM (GMT+0000)
Template Title:	Technical Report
Asset Groups:	SecurityLab
IPs:	-
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 04/10/2024
Active Hosts:	2
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	Security Risk (Avg)	Business Risk
6	2.7	13/100

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	4	-	-	4
2	2	-	-	2
1	0	-	-	0
Total	6	-	-	6

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
SMB / NETBIOS	4	-	-	4
TCP/IP	1	-	-	1
General remote services	1	-	-	1
Total	6	-	-	6

Ilustración 37 Sumario de vulnerabilidades generado por Qualys

La ilustración 38 exhibe un gráfico de barras que ilustra el nivel de riesgo una vez que se han corregido las vulnerabilidades mencionadas en el informe anterior. Este gráfico proporciona una representación visual clara y concisa de la gravedad de las vulnerabilidades. Además, se nota que el riesgo ha disminuido significativamente después de aplicar las correcciones.

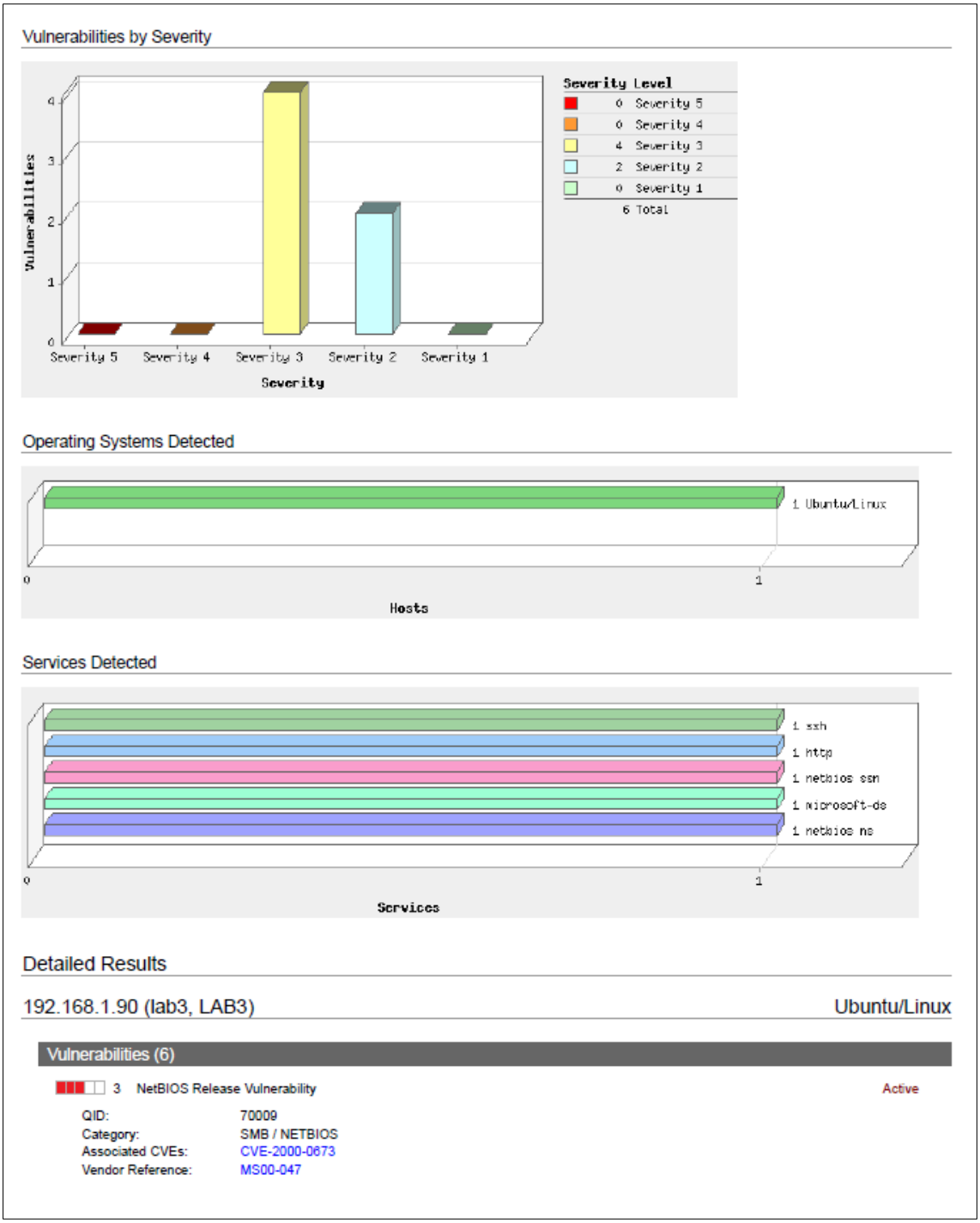
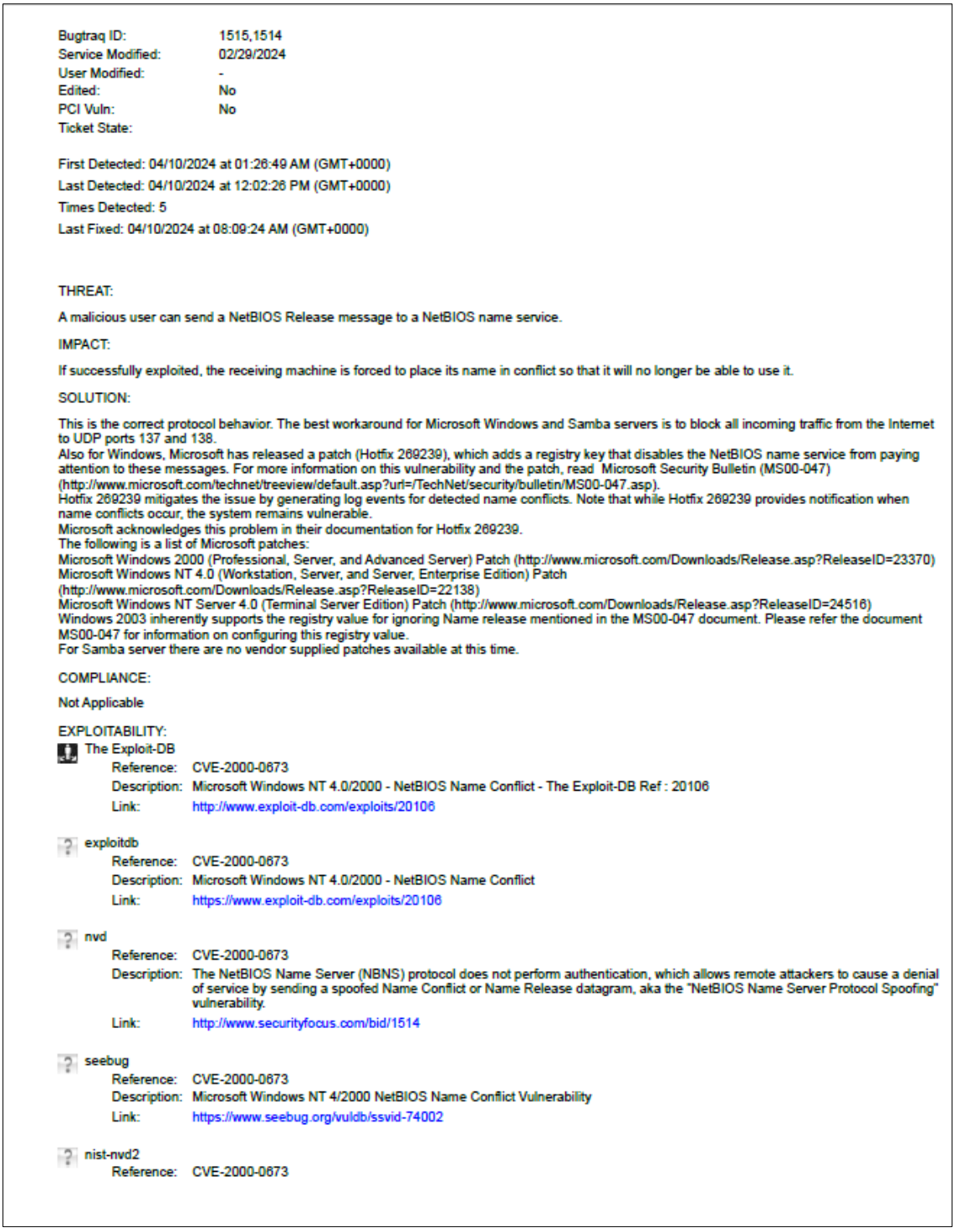


Ilustración 38 Gráfico de barras con los niveles de seguridad

La ilustración 39 nos muestra una vulnerabilidad que se produce debido a la version de NetBios, en la cual se puede enviar paquetes de mensajeria hacia un servicio de la BIOS, en el caso de que esta vulnerabilidad sea explotada se bloquearan servicios. Como solución recomendada por el informe la mejor manera para solventar esta exploit es bloquear el tráfico entrante proveniente de internet hacia los puertos 137 y 138.



Bugtraq ID: 1515,1514
Service Modified: 02/29/2024
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)
Last Detected: 04/10/2024 at 12:02:26 PM (GMT+0000)
Times Detected: 5
Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

A malicious user can send a NetBIOS Release message to a NetBIOS name service.

IMPACT:

If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.

SOLUTION:

This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and 138.
Also for Windows, Microsoft has released a patch (Hotfix 269239), which adds a registry key that disables the NetBIOS name service from paying attention to these messages. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable.
Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows 2000 (Professional, Server, and Advanced Server) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23370)
Microsoft Windows NT 4.0 (Workstation, Server, and Server, Enterprise Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22138)
Microsoft Windows NT Server 4.0 (Terminal Server Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24516)
Windows 2003 inherently supports the registry value for ignoring Name release mentioned in the MS00-047 document. Please refer the document MS00-047 for information on configuring this registry value.
For Samba server there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link: http://www.exploit-db.com/exploits/20106

exploitdb
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict
Link: https://www.exploit-db.com/exploits/20106

nvd
Reference: CVE-2000-0673
Description: The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.
Link: http://www.securityfocus.com/bid/1514

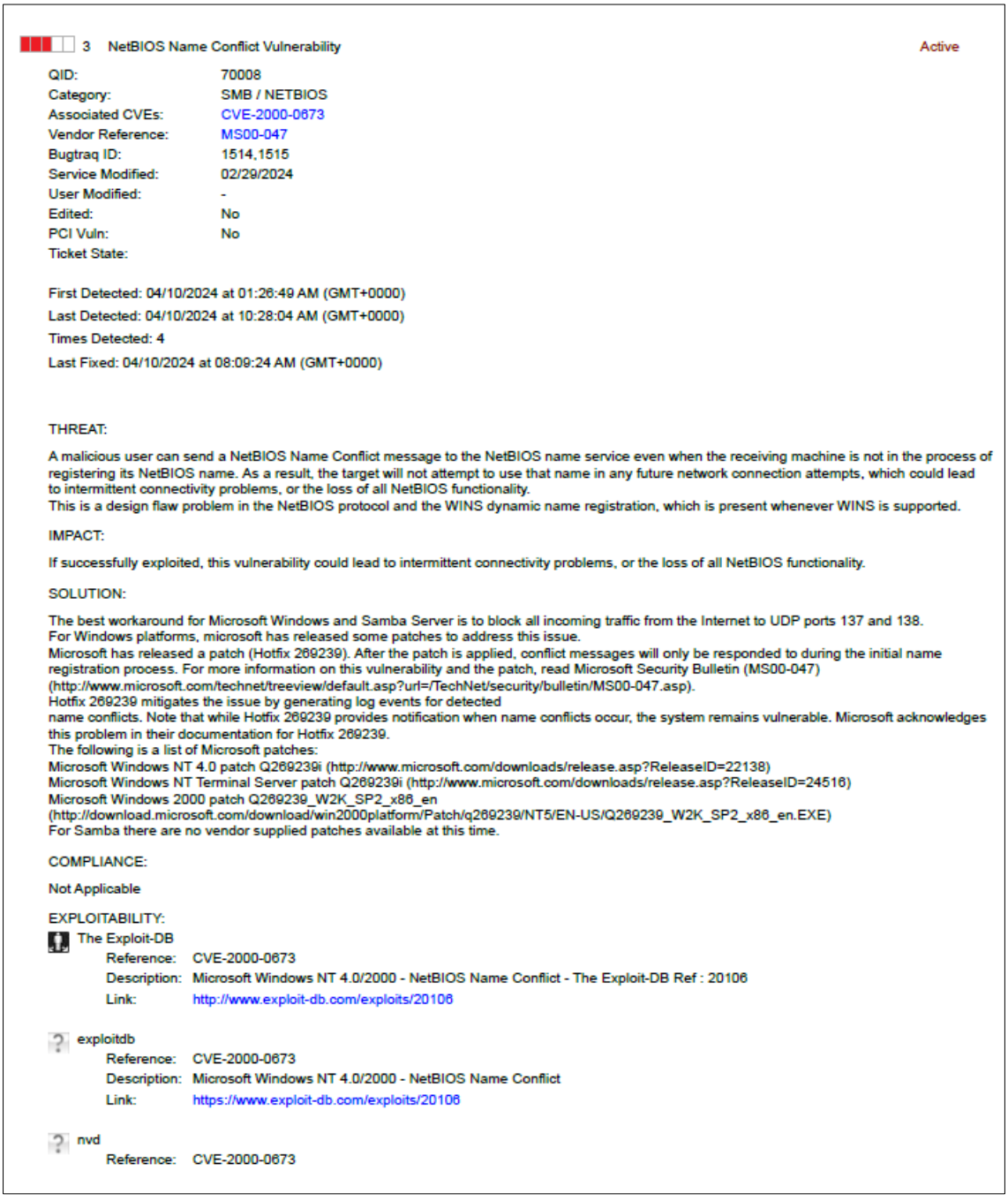
seebug
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4/2000 NetBIOS Name Conflict Vulnerability
Link: https://www.seebug.org/vuldb/ssvid-74002

nist-nvd2
Reference: CVE-2000-0673

Ilustración 39 Vulnerabilidad de NetBIOS

La ilustración 40 nos indica un exploit en la resolucion de nombres de la BIOS, debido a que un individuo malintencionado tiene la capacidad de enviar un mensaje de conflicto de nombres NetBIOS al servicio de nombres, incluso cuando la máquina receptora no está en el proceso de registrar el nombre. Como resultado, el objetivo no intentará utilizar ese nombre en futuras conexiones a la red, lo que podría ocasionar problemas de conectividad intermitentes o incluso la pérdida total de funcionalidad NetBIOS. Este problema radica en una falla de diseño en el protocolo NetBIOS y el registro dinámico de

nombres WINS, y se presenta siempre que se admita WINS.. Como solución recomendada por el informe la mejor manera para solventar esta exploit es bloquear el tráfico entrante proveniente de internet hacia los puertos 137 y 138.



3 NetBIOS Name Conflict Vulnerability — Active

QID:	70008
Category:	SMB / NETBIOS
Associated CVEs:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1514,1515
Service Modified:	02/29/2024
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 04/10/2024 at 01:26:49 AM (GMT+0000)
Last Detected: 04/10/2024 at 10:28:04 AM (GMT+0000)
Times Detected: 4
Last Fixed: 04/10/2024 at 08:09:24 AM (GMT+0000)

THREAT:

A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, the target will not attempt to use that name in any future network connection attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.
This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.

IMPACT:

If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

SOLUTION:

The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.
For Windows platforms, microsoft has released some patches to address this issue.
Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected
name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows NT 4.0 patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=22138)
Microsoft Windows NT Terminal Server patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=24516)
Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en
(http://download.microsoft.com/download/win2000platform/Patch/q269239/NT5/EN-US/Q269239_W2K_SP2_x86_en.EXE)
For Samba there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

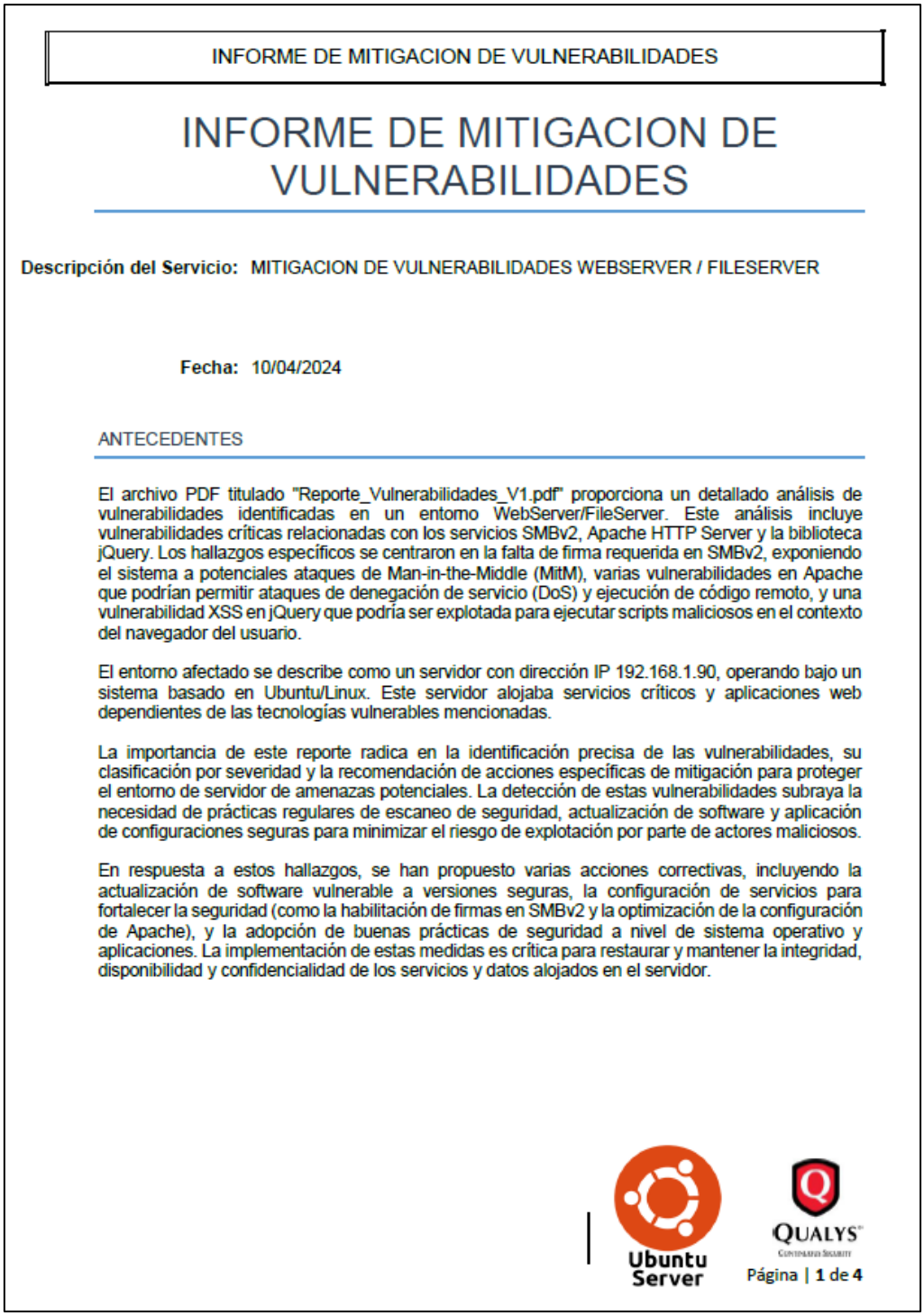
The Exploit-DB
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link: http://www.exploit-db.com/exploits/20106

exploitdb
Reference: CVE-2000-0673
Description: Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict
Link: https://www.exploit-db.com/exploits/20106

nvd
Reference: CVE-2000-0673

Ilustración 40 Vulnerabilidad de NetBIOS en conflicto de nombres

Anexo 3: Informe de Mitigación de Vulnerabilidades



INFORME DE MITIGACION DE VULNERABILIDADES

INFORME DE MITIGACION DE VULNERABILIDADES

Descripción del Servicio: MITIGACION DE VULNERABILIDADES WEBSERVER / FILESERVER

Fecha: 10/04/2024

ANTECEDENTES

El archivo PDF titulado "Reporte_Vulnerabilidades_V1.pdf" proporciona un detallado análisis de vulnerabilidades identificadas en un entorno WebServer/FileServer. Este análisis incluye vulnerabilidades críticas relacionadas con los servicios SMBv2, Apache HTTP Server y la biblioteca jQuery. Los hallazgos específicos se centraron en la falta de firma requerida en SMBv2, exponiendo el sistema a potenciales ataques de Man-in-the-Middle (MitM), varias vulnerabilidades en Apache que podrían permitir ataques de denegación de servicio (DoS) y ejecución de código remoto, y una vulnerabilidad XSS en jQuery que podría ser explotada para ejecutar scripts maliciosos en el contexto del navegador del usuario.

El entorno afectado se describe como un servidor con dirección IP 192.168.1.90, operando bajo un sistema basado en Ubuntu/Linux. Este servidor alojaba servicios críticos y aplicaciones web dependientes de las tecnologías vulnerables mencionadas.

La importancia de este reporte radica en la identificación precisa de las vulnerabilidades, su clasificación por severidad y la recomendación de acciones específicas de mitigación para proteger el entorno de servidor de amenazas potenciales. La detección de estas vulnerabilidades subraya la necesidad de prácticas regulares de escaneo de seguridad, actualización de software y aplicación de configuraciones seguras para minimizar el riesgo de explotación por parte de actores maliciosos.

En respuesta a estos hallazgos, se han propuesto varias acciones correctivas, incluyendo la actualización de software vulnerable a versiones seguras, la configuración de servicios para fortalecer la seguridad (como la habilitación de firmas en SMBv2 y la optimización de la configuración de Apache), y la adopción de buenas prácticas de seguridad a nivel de sistema operativo y aplicaciones. La implementación de estas medidas es crítica para restaurar y mantener la integridad, disponibilidad y confidencialidad de los servicios y datos alojados en el servidor.

Ubuntu Server

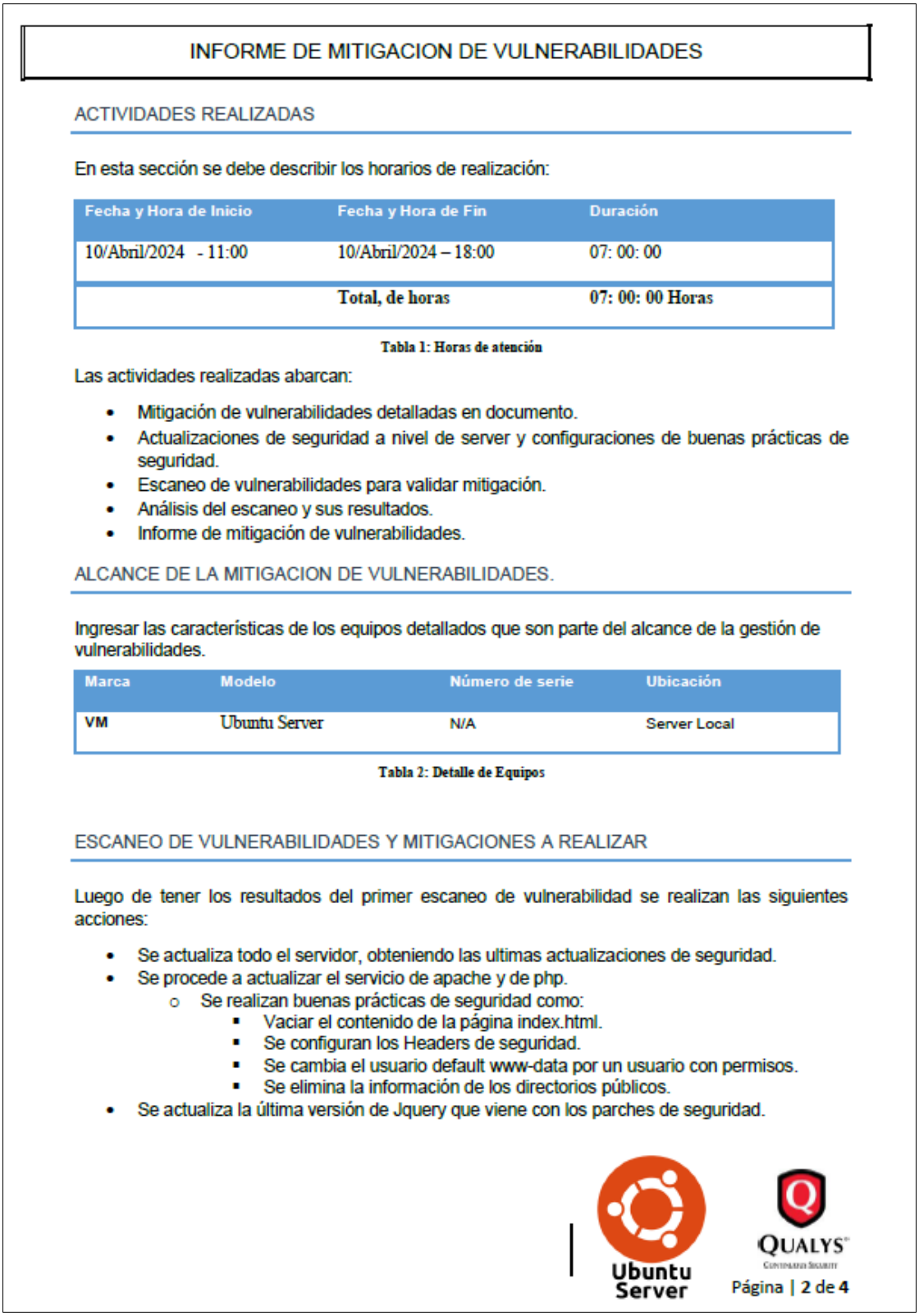
QUALYS

Página | 1 de 4

Ilustración 41 Antecedentes del reporte de mitigación

En la Ilustración 42 se presentan en detalle las acciones planificadas para abordar las vulnerabilidades y el alcance previsto de estas medidas. Además, se especifica el equipo responsable de llevar a cabo la verificación y se establece el plazo de ejecución para garantizar una implementación efectiva y oportuna de las acciones de mitigación. Esta ilustración proporciona una visión completa del proceso planificado para abordar las

vulnerabilidades identificadas, asegurando una respuesta organizada y coordinada para fortalecer la seguridad del sistema.



INFORME DE MITIGACION DE VULNERABILIDADES

ACTIVIDADES REALIZADAS

En esta sección se debe describir los horarios de realización:

Fecha y Hora de Inicio	Fecha y Hora de Fin	Duración
10/Abril/2024 - 11:00	10/Abril/2024 – 18:00	07: 00: 00
	Total, de horas	**07: 00: 00 Horas**

Tabla 1: Horas de atención

Las actividades realizadas abarcan:

- Mitigación de vulnerabilidades detalladas en documento.
- Actualizaciones de seguridad a nivel de server y configuraciones de buenas prácticas de seguridad.
- Escaneo de vulnerabilidades para validar mitigación.
- Análisis del escaneo y sus resultados.
- Informe de mitigación de vulnerabilidades.

ALCANCE DE LA MITIGACION DE VULNERABILIDADES.

Ingresar las características de los equipos detallados que son parte del alcance de la gestión de vulnerabilidades.

Marca	Modelo	Número de serie	Ubicación
VM	Ubuntu Server	N/A	Server Local

Tabla 2: Detalle de Equipos

ESCANEO DE VULNERABILIDADES Y MITIGACIONES A REALIZAR

Luego de tener los resultados del primer escaneo de vulnerabilidad se realizan las siguientes acciones:

- Se actualiza todo el servidor, obteniendo las ultimas actualizaciones de seguridad.
- Se procede a actualizar el servicio de apache y de php.
  - Se realizan buenas prácticas de seguridad como:
    - Vaciar el contenido de la página index.html.
    - Se configuran los Headers de seguridad.
    - Se cambia el usuario default www-data por un usuario con permisos.
    - Se elimina la información de los directorios públicos.
- Se actualiza la última versión de Jquery que viene con los parches de seguridad.

Ubuntu Server

QUALYS

Página | 2 de 4

Ilustración 42 Actividades realizadas y alcance de la mitigación de vulnerabilidades

En las Ilustraciones 43 y 44 se describen detalladamente las acciones que deben llevarse a cabo, así como la verificación de los resultados después de la implementación de las medidas de mitigación. Además, se presentan conclusiones importantes que resaltan la importancia de mantener buenas prácticas de seguridad en el sistema. Estas

ilustraciones proporcionan una guía paso a paso para garantizar la efectividad de las medidas de seguridad implementadas y para asegurar la integridad y protección del sistema frente a posibles amenazas y vulnerabilidades.

INFORME DE MITIGACION DE VULNERABILIDADES

- A nivel de SMB:
  - Se actualiza la información del archivo de configuración smb.conf

```
[CarpetaCompartida]
path = /srv/samba/CarpetaCompartida
browseable = yes
writable = no
guest ok = no
read only = yes
valid users = usuario1, usuario2
```

  -
  - En la nueva configuración se cambia la ubicación del directorio y los permisos de acceso a usuarios restringidos.
  - Se aseguró el servicio SMB aplicando firmas digitales a los paquetes, limitando la exposición a ataques.

```
[global]

server signing = mandatory
client signing = mandatory
```

  -

ACCIONES A REALIZAR

Se solicita realizar un segundo escaneo el cual validara la mitigación de las vulnerabilidades. El nombre del documento será "**Reporte_Vulnerabilidades_V2.pdf**". Luego del mismo se procedería a revisar los resultados y mitigar los resultados nuevos o en su caso crear un documento de SRA.

CONCLUSIÓN

Tras la implementación rigurosa de las acciones de mitigación detalladas y la adopción de buenas prácticas de seguridad en respuesta a las vulnerabilidades identificadas en el informe "**Reporte_Vulnerabilidades_V1.pdf**", se ha mejorado significativamente la postura de seguridad del entorno de servidor WebServer/FileServer. Las medidas adoptadas abordaron de manera efectiva las vulnerabilidades críticas asociadas con los servicios SMBv2, Apache HTTP Server, y la biblioteca jQuery, además de actualizar componentes clave del sistema como PHP y MySQL a versiones más seguras y configurar adecuadamente los parámetros de seguridad para Apache2.

Las vulnerabilidades que se registran en el documento "**Reporte_Vulnerabilidades_V2.pdf**" son consideradas falsos positivos por lo que se procede a aceptar el riesgo a través de un SRA.

La actualización de Apache y la eliminación de versiones obsoletas y vulnerables del software aseguran que el servidor está protegido contra explotaciones conocidas que podrían comprometer la integridad y disponibilidad de los servicios web. La implementación de una configuración segura para SMBv2 mitiga el riesgo de ataques de Man-in-the-Middle, protegiendo así la comunicación entre el servidor y los clientes. La actualización de jQuery a su última versión aborda vulnerabilidades específicas de XSS, mejorando la seguridad de las aplicaciones web frente a ataques de inyección de scripts.

Ubuntu Server

QUALYS

Página | 3 de 4

Ilustración 43 Acciones a realizar para la mitigación de vulnerabilidades

INFORME DE MITIGACION DE VULNERABILIDADES

Adicionalmente, la adopción de buenas prácticas de seguridad, como la configuración de encabezados de seguridad en Apache, contribuye a un entorno más robusto y resiliente ante ataques. Estas medidas no solo corrigen las deficiencias identificadas, sino que también promueven una cultura de seguridad proactiva, donde la prevención y la detección temprana de vulnerabilidades son prioritarias.

Es crucial reconocer que la seguridad de los sistemas informáticos es un proceso continuo y dinámico. Aunque las acciones tomadas han mejorado notablemente la seguridad del sistema, es esencial mantener una vigilancia constante y realizar evaluaciones periódicas de seguridad para identificar y mitigar nuevas vulnerabilidades que puedan surgir. La implementación de políticas de actualización de software, monitoreo de seguridad, y educación continua sobre las mejores prácticas de seguridad son fundamentales para sostener y mejorar la postura de seguridad del sistema a largo plazo.

En conclusión, el sistema ahora se considera significativamente más seguro como resultado de las acciones de mitigación implementadas. Sin embargo, la seguridad del sistema requiere un compromiso constante con las prácticas recomendadas y una respuesta ágil a las nuevas amenazas de seguridad.

DOCUMENTOS

Nombre Archivo	Versión	Fecha Creación
Reporte_Vulnerabilidades_V1.pdf	Versión 1	10 abril 2024
Reporte_Vulnerabilidades_V2.pdf	Versión 1	10 abril 2024

Ubuntu Server

QUALYS

Página | 4 de 4

Ilustración 44 Conclusiones del reporte de mitigación

Anexo 5: Documento de aceptación del riesgo

La Ilustración 45 muestra el documento de aceptación de riesgos, en el que se especifican las vulnerabilidades que han sido identificadas como falsos positivos. En este contexto, los exploits mencionados en el informe no representan ninguna amenaza real para la estabilidad del sistema. Es decir, aunque inicialmente se identificaron como posibles riesgos, tras un análisis más detallado se determinó que no constituyen una vulnerabilidad genuina. Este documento es crucial para documentar y gestionar adecuadamente los riesgos de seguridad, garantizando que los recursos se asignen de manera efectiva y que se prioricen las acciones de mitigación según la verdadera naturaleza de las amenazas.

DOCUMENTO DE ACEPTACIÓN DE RIESGO DE SEGURIDAD

DOCUMENTO DE ACEPTACIÓN DE RIESGO DE SEGURIDAD

Fecha: 10/04/2024

DESCRIPCIÓN DEL ENTORNO

IP del Host: 192.168.1.90

Nombre del Host: LAB 3

Sistema Operativo: Ubuntu/Linux

RESUMEN DE VULNERABILIDADES ACEPTADAS.

ID de Vulnerabilidad	Descripción	Severidad
82054	TCP Sequence Number Approximation Based Denial of Service	3
70009	NetBIOS Release Vulnerability	3

RACIONALIZACIÓN PARA LA ACEPTACIÓN DEL RIESGO

Justificación para la Aceptación: Las vulnerabilidades fueron reconocidas y aceptadas tras haber sido efectivamente mitigadas previamente. La más reciente detección registrada en el informe tuvo lugar el 04/10/2024 a las 12:02:26 PM. Estos resultados sugieren que las vulnerabilidades detectadas inicialmente pueden haber sido interpretadas erróneamente como tales, siendo más bien falsos positivos.

Fecha de la Próxima Revisión: 06/10/2024

DOCUMENTOS

Nombre Archivo	Versión	Fecha Creación
Reporte_Vulnerabilidades_V2.pdf	Versión 1	10 abril 2024

FIRMAS

Realizado	Cargo	Fecha

Ubuntu Server

QUALYS

Página | 1 de 1

Ilustración 45 Resumen del documento de aceptación