

Análisis y evaluación de vulnerabilidades en servidor Linux de monitoreo de red de la Universidad del Externado

Jonathan Arley Vargas Sánchez, Luis Francisco Terreros Pardo y Anderson Steve Raba Enciso

Especialización en Seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado

Jaime Andrés Chaparro Sanchez

27 de mayo de 2021



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional

Análisis y evaluación de vulnerabilidades en servidor Linux de monitoreo de red de la Universidad del Externado

Autor(es):
Jonathan Arley Vargas Sánchez
Luis Francisco Terreros Pardo
Anderson Steve Raba Enciso

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad informática

Director (a):

Título (Ph.D., M.Sc., M.Eng, Ingeniero(a), etc.) y nombre del director(a)

Codirector (a):

Línea de Investigación:

Nombrar la línea de investigación en la que se enmarca el trabajo de investigación

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

2024

Resumen

El siguiente proyecto es el resultado del análisis y evaluación de riesgos sobre el servidor Linux de monitoreo de red de la universidad del externado, determinando el nivel de riesgo, las amenazas, las vulnerabilidades, los controles implementados y sus respectivas recomendaciones de seguridad.

En primera instancia se hizo una valoración del activo, se evaluaron los impactos a los cuales está expuesto dentro de la universidad, en donde se identificó el responsable del servicio y la criticidad, posterior se realizó un análisis a la situación actual del activo, identificando los controles existentes de seguridad y su estado en la gestión del riesgo en la seguridad de la información, enseguida se determinaron las fallas y vulnerabilidades para finalmente definir las recomendaciones necesarias para reducir la superficie de ataque.

Palabras clave: seguridad de la información, superficie de ataque, riesgo.

Abstract

The following project is the result of the risk analysis and evaluation of the Linux network monitoring server of the externship university, determining the level of risk, threats, vulnerabilities, implemented controls and their respective security recommendations.

In the first instance, an assessment of the asset was made, the impacts to which it is exposed within the university were evaluated, where the person responsible for the service and the criticality were identified, subsequently an analysis was carried out of the current situation of the asset, identifying the existing security controls and their status in information security risk management, the flaws and vulnerabilities were immediately determined to finally define the necessary recommendations to reduce the attack surface.

Keywords: information security, attack surface, risk.

Contenido

PÁG.

RESUMEN ¡ERROR! MARCADOR NO DEFINIDO.

INTRODUCCIÓN ¡ERROR! MARCADOR NO DEFINIDO.

ANTECEDENTES Y JUSTIFICACIÓN **¡ERROR! MARCADOR NO DEFINIDO.**
FORMULACIÓN DEL PROBLEMA 3
OBJETIVO GENERAL **¡ERROR! MARCADOR NO DEFINIDO.**
Objetivos Específicos ***¡Error! Marcador no definido.***
ALCANCES Y LIMITACIONES 4

1. MARCO TEÓRICO ¡ERROR! MARCADOR NO DEFINIDO.

2. DISEÑO METODOLÓGICO ¡ERROR! MARCADOR NO DEFINIDO.

3. RESULTADOS **8**

4. CONCLUSIONES Y RECOMENDACIONES ¡ERROR! MARCADOR NO DEFINIDO.**9**

4.1 CONCLUSIONES **¡ERROR! MARCADOR NO DEFINIDO.**9
4.2 RECOMENDACIONES 20

5. ANEXOS ¡ERROR! MARCADOR NO DEFINIDO.**2**

BIBLIOGRAFÍA **23**

Introducción

En la actualidad las instituciones educativas y todo el sector empresarial está acogiendo las tecnologías de la información como el medio para organizar y acceder a los datos, esto es beneficioso pero a su vez aumenta los problemas de seguridad, los riesgos asociados son latentes y las amenazas se multiplican, es necesario que las organizaciones tomen conciencia de lo importante de proteger o conservar los pilares fundamentales de la seguridad de la información, pasar por alto el tema podría ocasionar daños importantes, generando perdidas a nivel económico, social y estructural para la organización.

De acuerdo con lo anterior es necesario tener un modelo de seguridad de la información en el cual se establezcan estrategias, políticas, procedimientos y medidas de seguridad con el objeto de proteger la información, partiendo de la seguridad física y lógica, evitando el robo, la manipulación y el acceso no autorizado de la información.

Por esta razón, es importante adoptar de manera correcta las medidas adecuadas y actualizadas generando bases sólidas de seguridad, preparando a las organizaciones contra ciberataques, amenazas internas, desastres naturales y errores humanos.

Antecedentes

La Universidad del Externado es reconocida a nivel nacional como una de las 10 mejores instituciones por sus grandes logros académicos, manteniendo su prestigiosa reputación como una institución de excelencia comprometida con la formación integral de sus estudiantes. Además, promueve actividades que permiten a toda su comunidad aprovechar el tiempo libre, disfrutar del esparcimiento, participar en diversas actividades deportivas y promover la salud, fomentando la convivencia y la cultura ciudadana.

En un momento determinado, se implementó un sistema de monitoreo para recopilar información sobre el comportamiento de la red en tiempo real. Sin embargo, es posible que en ese momento no se hayan considerado los riesgos que esto podría implicar en términos de seguridad, ya que el sistema administra información sensible que no debería estar en riesgo frente a posibles ataques cibernéticos. Aunque se han implementado algunos controles, no son suficientes, por lo que es necesario cambiar los sistemas o aplicar medidas correctivas adicionales.

Justificación

Las instituciones educativas se han vuelto un blanco para los cibercriminales debido al manejo de grandes cantidades de información sensible, como la información financiera, sistemas académicos (estudiantes, docentes) y proyectos de investigación, con el propósito de obtener dinero, hacer espionaje o realizar estafas, además de no contar con el personal ni con las estrategias de seguridad adecuadas de prevención ante amenazas por niveles bajo de inversión en ciberseguridad.

Según el reporte de seguridad realizado por Check Point, el sector educativo fue el más atacado en el primer semestre del 2023 con un promedio de amenaza de 2000 intentos por semana, esto es algo no muy alentador para las instituciones educativas. (Maya. 2023)

En el 2023, el panorama de la ciberseguridad aumento de una manera descomunal con respecto a ataques de ransomware, representando el 10% de todos los tipos de malware detectados por Check Point, "casi la mitad de todos los incidentes que manejaron involucraron ransomware y el número reportado de víctimas de ransomware llegó a casi 5.000 víctimas, un

marcado aumento con respecto a las 2.600 reportadas en 2022". sin dejar atrás los vectores de infección principales como los ataques basados en correo electrónico, el 88% de las entregas de archivos maliciosos se realizan a través de este medio y el restante se descarga directamente desde internet, igualmente la suplantación de identidad, phishing, deepfake y la fuga de datos. (Maya. 2023)

Sophos en su reporte anual en el periodo 2023, revelo que el índice de ataques de ransomware al sector educativo sigue en aumento. "El 80 % de las instituciones de educación primaria y el 79 % de las instituciones de educación superior afirmaron haber sido víctimas del ransomware en el último año, comparado con el 56 % y el 64 %, respectivamente, de nuestra encuesta del 2022". (Sophos, 2023)

Formulación del Problema

¿Cuáles son los riesgos que inciden al no implementar las medidas de seguridad adecuadas para el servidor Linux de monitoreo de red?

Objetivo General

Evaluar el estado de seguridad del servidor Linux de monitoreo de red de la universidad.

Objetivos Específicos

- Establecer una metodología para la identificación del activo y estimación del riesgo.
- Determinar el tratamiento de los riegos, identificando los controles y la situación actual.
- Realizar un análisis de vulnerabilidades con una herramienta de seguridad informática, para identificar las superficies de ataque.
- Elaborar recomendaciones para reducir o eliminar el riesgo de acuerdo con las fallas y vulnerabilidades encontradas.

Alcances y Limitaciones

Alcances

A continuación, se listan los alcances necesarios que se tuvieron en cuenta en el proyecto:

- Análisis y evaluación de riesgos del servidor Linux de monitoreo de red de la universidad.
- Análisis de vulnerabilidades del servidor Linux de monitoreo de red de la universidad.
- Se enfocaron las pruebas en caja blanca.
- Propuesta de medidas correctivas o de mitigación para resolver las vulnerabilidades identificadas.

Limitaciones

- No se considera la explotación de vulnerabilidades sobre el activo, se entregan las respectivas recomendaciones con el fin de que sean analizadas, aprobadas y ejecutadas.
- No se puede realizar análisis a otro dispositivo que no esté dentro del alcance.
- No utilizar nombre propio en documento.
- No se cuenta con la disponibilidad del activo, lo que fue necesario con el administrador establecer horarios para las pruebas.

1. Marco teórico

En la actualidad los activos de información son el punto clave de las organizaciones, son aquellos recursos utilizados para desarrollar las operaciones diarias y cumplir con los objetivos estratégicos establecidos, por lo tanto, es fundamental adoptar un sistema de gestión para la información garantizando la disponibilidad, confidencialidad e integridad, con esto garantizamos la continuidad del negocio ante amenazas inminentes.

Con la finalidad de garantizar los objetivos de la seguridad de la información, la norma ISO27001 se ha convertido en un marco referente para las organizaciones en el tema de gestión de la seguridad, va dirigida a todo tipo de empresa sin importar el tamaño o su actividad económica y evalúa las vulnerabilidades que pueden afectar los activos de información, y donde se define lo necesario para evitar que las amenazas produzcan daños graves a la organización. (ISO 27001. n.d)

Para que esto se cumpla satisfactoriamente es necesario aparte de la identificación de los activos y su nivel de criticidad hacer el análisis del riesgo, cuantitativo y cualitativo donde nos permita hacer una valoración más certera acerca del riesgo que pueden afectar los activos de la organización, esto implica validar el nivel de riesgo al que este asociado, establecer criterios de razonabilidad, como aquello que la organización está dispuesto a tolerar o que permita el avance normal de las operaciones del proceso responsable del riesgo, es decir su valor mínimo tolerable, teniendo en cuenta que al implementar una cierta cantidad de controles no se garantiza eliminar el riesgo por completo, con esta evaluación se pretende establecer probabilidades, vulnerabilidades e impactos sobre los activos de información.

Una gestión eficiente del riesgo está relacionada con la mejora continua, el ciclo PHVA es una estrategia de cuatro pasos (planear - hacer - verificar - actuar y es muy utilizado

para la gestión de la seguridad de la información, dando resultados positivos a las organizaciones en temas de costos, optimizando la productividad, reduciendo precios e incrementando la participación en el mercado, mejorando así continuamente por la retroalimentación del paso final a la inicial. (ISO 27001. n.d)

El pentesting ha tomado fuerza gracias a las consecuencias resultantes de los ataques diarios a los sistemas en las diferentes organizaciones en donde se ven reflejadas pérdidas económicas gigantescas y una reputación por el piso, son un conjunto de herramientas para evaluar la seguridad de los sistemas, hay diversas metodologías de pentesting cada una desarrollada para ámbitos diferentes, como por ejemplo la ethical hacking y se refiere a una secuencia de pasos que como resultado llevan a evaluar todos los puntos de entrada y vulnerabilidades posibles, en conclusión es una metodología muy completa para auditorias técnicas de seguridad y complementa con los estándares y buenas prácticas de las normas establecidas como la ISO27001, siendo ideal para aplicar las pruebas de seguridad de la información a las organizaciones. (Veloz, J n.d)

2. Diseño Metodológico

Para el desarrollo del proyecto se emplea el ciclo PHVA (planear - hacer - verificar - actuar) para la mejora continua en el desarrollo de las actividades de la universidad, esto con el fin de que se incorpore como buenas prácticas, para la gestión del riesgo se toman las pautas contempladas en la guía de seguridad del Ministerio de las Tecnologías de la Información y las Comunicaciones, la norma ISO27001/27005 y la metodología del ethical hacking brindando estrategias para mitigar o eliminar todo clase de riesgo evitando pérdidas de información.

3. Resultados

3.1. Etapa 1 - Planear

Para identificar, clasificar y valorar el activo, se tomó en cuenta lo basado en la norma ISO 27005 y lo sugerido por el Ministerio de Tecnologías de la Información y las Comunicaciones, tomando como referencia los objetivos de la seguridad de la información (confidencialidad, integridad y disponibilidad) tal como se describe en el anexo A.

3.2. Etapa 2 - Hacer

Se hace el levantamiento de información inicial sobre el activo de manera detallada, el cual contempla: (clasificación, descripción, responsable, ubicación, entre otros aspectos relevantes) con ayuda del administrador de red. generando el recurso base para el desarrollo de las actividades.

Identificación de activo de información						
Numero de activo	Proceso macro	Tipo de activo	Nombre del activo	Descripción del activo	Ubicación	Responsable
R3 - 48	Infraestructura	Software - VM - VMware	Servidor Linux - Ubuntu Dashboard	Recolección de información de la red LAN y WLAN, en graficas.	Data center	Administrador de redes

Tabla1. Identificación de activo

Valoración de activo de información							
Numero de activo	Nombre del activo	Tipo de soporte	Ubicación	C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
R3 - 48	Servidor Linux - Ubuntu Dashboard	Lógico	Data center	3	3	3	3

Tabla 2. Valoración de activo

Teniendo el impacto sobre el activo, se realiza la identificación de amenazas, vulnerabilidades y controles existentes, esto con el fin de determinar el nivel de riesgo.

Proceso	Numero de activo	Nombre del activo	Amenaza
Infraestructura	R3 - 48	Servidor Linux - Ubuntu Dashboard	Indisponibilidad de servicio
			Uso no autorizado del equipo
			Corrupción de datos
			Mal funcionamiento del software
			Error en el uso
			Incumplimiento en el mantenimiento del sistema de información
			Falla del equipo

Tabla 3. Identificación de amenazas

Proceso	Numero de activo	Nombre del activo	Amenaza	Controles implementados existentes
Infraestructura	R3 - 48	Servidor Linux - Ubuntu Dashboard	Indisponibilidad de servicio	No
			Uso no autorizado del equipo	Soporte contratado
			Corrupción de datos	No
			Mal funcionamiento del software	No
			Error en el uso	Soporte contratado con el desarrollador
			Incumplimiento en el mantenimiento del sistema de información	No
			Falla del equipo	No

Tabla 4. Identificaciones de controles existentes

Para la identificación y evaluación de vulnerabilidades se tiene en cuenta la metodología de ethical hacking contemplado de la siguiente manera:

3.2.1. Definición del alcance

La estrategia o enfoque está basado en pruebas de caja blanca, donde se evaluará un sistema en específico, todas las pruebas se centraron en el objetivo aprobado, a continuación, se enumera el sistema en el ámbito de las pruebas:

Objetivo	Descripción
IP 10.x.x.x	Servidor Linux - Ubuntu Dashboard

Tabla 6. Activo aprobado

3.2.2. Escaneo

Para el escaneo, se conectó el equipo auditor (Kali Linux) a la red de la universidad, con herramientas automatizadas como Nmap, se procede a un escaneo completo con la IP del objetivo, identificando información importante como sistema operativo, puertos abiertos, servicios que se están ejecutando, entre otros.

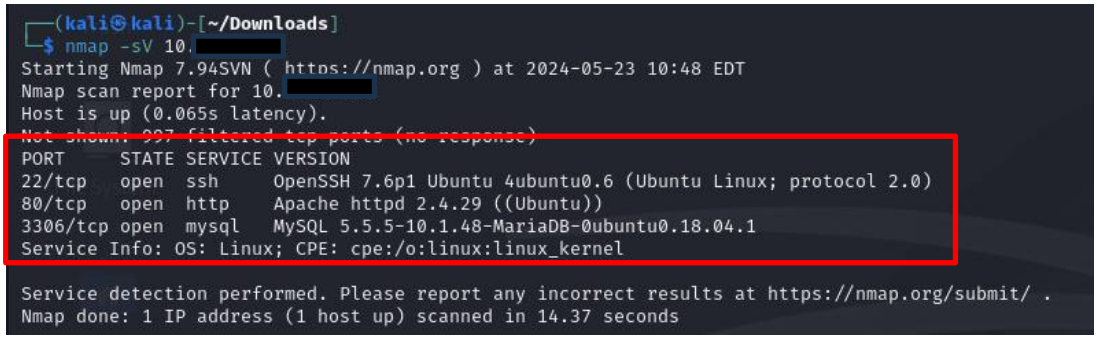


Figura 1. Nmap – Escaneo

Posterior se hace un escaneo de vulnerabilidades con la herramienta Nessus y Nmap, en donde se evidencia un listado con todas las vulnerabilidades encontradas y su clasificación por severidad, cotejando así el resultado con bases de datos de vulnerabilidades. (CVE-details, 2024)

La correlación no siempre arroja resultados exitosos, por lo que también se generaron búsquedas manuales de acuerdo con los puertos, servicios y versiones del escaneo inicial.

A continuación, se enumeran las vulnerabilidades encontradas en el activo:

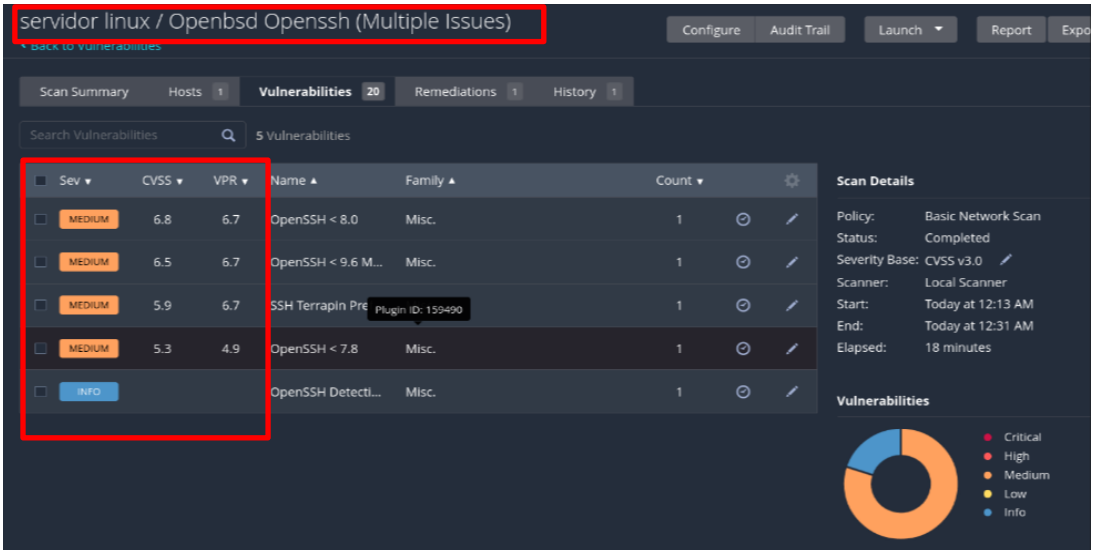


Figura 2. Nessus vulnerabilidades OpenSSH

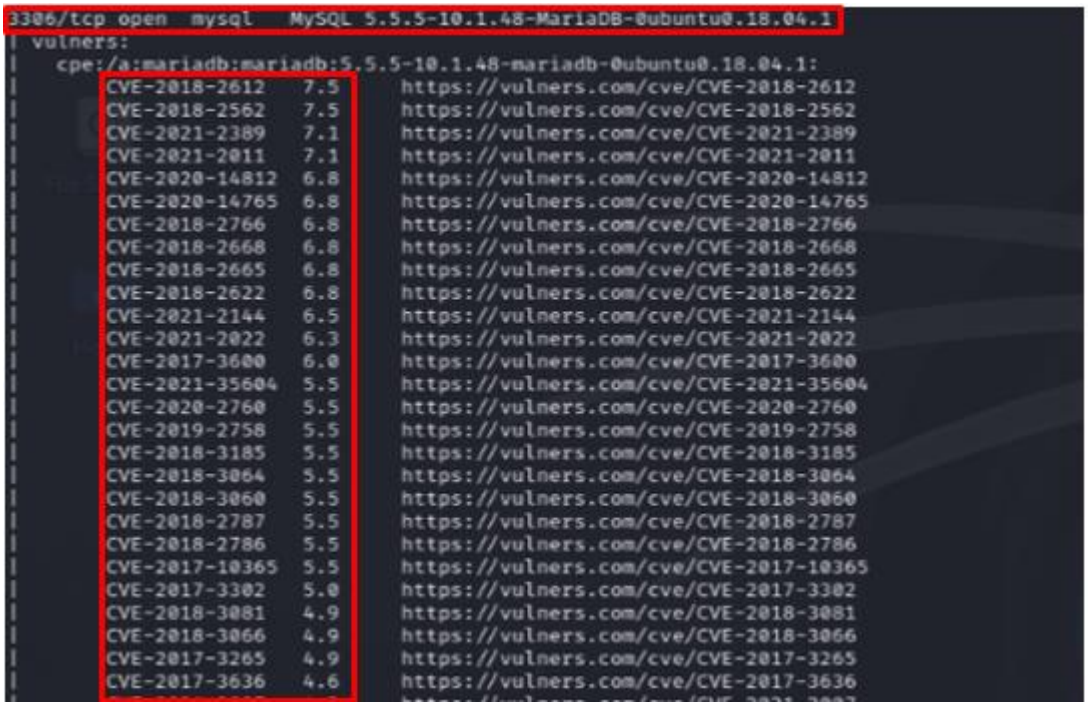


Figura 3. Nmap Vulnerabilidades MySQL

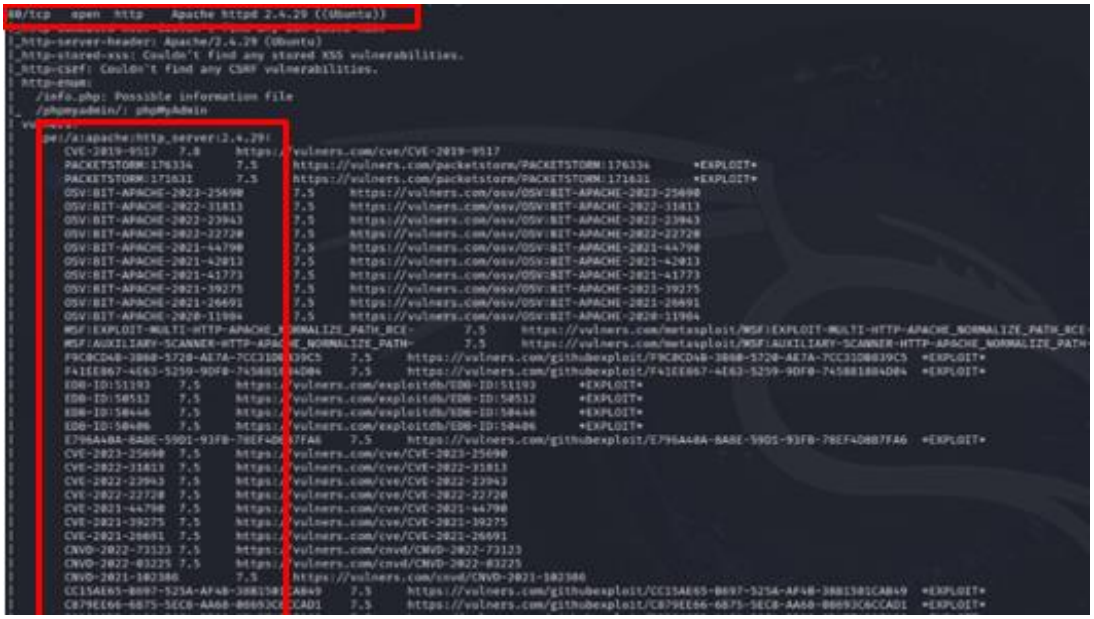


Figura 4. Nmap Vulnerabilidades Apache

3.3. Etapa 3 - Verificar

Se clasifican las vulnerabilidades encontradas, tomando como base el nivel de impacto y el reporte CVE, como se muestra continuación:

Vulnerabilidad CVE	Criticidad	Servicio	Descripción
CVE-2023-38408	Critica	OpenSSH	Tiene una ruta de búsqueda insuficientemente confiable, lo que lleva a la ejecución remota de código, afecta principalmente a los sistemas donde el agente SSH de OpenSSH está en uso y la función de reenvío del agente está habilitada.
CVE-2022-23943	Critica	Apache	La vulnerabilidad de escritura fuera de límites en mod_sed del servidor HTTP Apache permite a un atacante sobrescribir la memoria del montón con datos posiblemente proporcionados por el atacante. Este problema afecta a Apache HTTP Server 2.4 versión 2.4.52 y versiones anteriores.
CVE-2022-31813	Critica	Apache	Es posible que Apache HTTP Server 2.4.53 y versiones anteriores no envíen los encabezados X-Forwarded-* al servidor de origen según el mecanismo salto a salto del encabezado de conexión del lado del cliente. Esto se puede utilizar para omitir la autenticación basada en IP en el servidor/aplicación de origen.
CVE-2021-26691	Critica	Apache	En las versiones 2.4.0 a 2.4.46 del servidor Apache HTTP, un encabezado de sesión especialmente diseñado enviado por un servidor de origen podría provocar un desbordamiento
CVE-2020-15778	Alta	OpenSSH	En SSH en OpenSSH versiones hasta 8.3p1 permite una inyección de comandos en la función toremote de scp.c, como lo demuestran los caracteres backtick en el argumento de destino. NOTA: según se informa, el proveedor ha declarado que omite intencionadamente la validación de las "transferencias de argumentos anómalos" porque eso podría "tener grandes posibilidades de romper los flujos de trabajo existentes"
CVE-2019-0211	Alta	Apache	Existe una vulnerabilidad de escalada de privilegios en los scripts del módulo debido a la capacidad de ejecutar código arbitrario como proceso principal mediante la manipulación del marcador
CVE-2019-0217	Alta	Apache	Existe una vulnerabilidad de omisión de control de acceso en mod_auth_digest debido a una condición de carrera cuando se ejecuta en un servidor con subprocesos. Un atacante con credenciales válidas podría autenticarse utilizando otro nombre de usuario.
CVE-2020-13249	Alta	MySQL	libmariadb/mariadb_lib.c en MariaDB Connector/C anterior a 3.1.8 no valida correctamente el contenido de un paquete OK recibido de un servidor. NOTA: aunque mariadb_lib.c se basó

			originalmente en el código enviado para MySQL, este problema no afecta a ningún componente de MySQL compatible con Oracle
CVE-2017-15945	Alta	MySQL	Los scripts de instalación en los paquetes Gentoo dev-db/mysql, dev-db/mariadb, dev-db/percona-server, dev-db/mysql-cluster y dev-db/mariadb-galera anteriores al 29 de septiembre de 2017 tienen chown solicita árboles de directorios en los que el usuario puede escribir, lo que permite a los usuarios locales obtener privilegios aprovechando el acceso a la cuenta mysql para la creación de un enlace
CVE-2022-27387	Alta	Inyección SQL	Se descubrió que MariaDB Server v10.7 y versiones anteriores contenían un desbordamiento de búfer global en el componente decimal_bin_size, que se explota mediante declaraciones SQL especialmente diseñadas.
CVE-2023-5157	Alta	MySQL	Se encontró una vulnerabilidad en MariaDB. Un escaneo de puertos OpenVAS en los puertos 3306 y 4567 permite que un cliente remoto malicioso provoque una denegación de servicio.
CVE-2021-27928	Alta	MySQL	Se descubrió un problema de ejecución remota de código en MariaDB 10.2 anterior a 10.2.37, 10.3 anterior a 10.3.28, 10.4 anterior a 10.4.18 y 10.5 anterior a 10.5.9; Servidor Percona hasta el 3 de marzo de 2021; y el parche wsrep hasta el 3 de marzo de 2021 para MySQL. Una ruta de búsqueda que no es de confianza conduce a una inyección de evaluación, en la que un SUPERusuario de la base de datos puede ejecutar comandos del sistema operativo después de modificar wsrep_provider y wsrep_notify_cmd.
CVE-2021-41617	Alta	OpenSSH	Se encontró una falla en OpenSSH. Los programas auxiliares para AuthorizedKeysCommand y AuthorizedPrincipalsCommand pueden ejecutarse con privilegios asociados con membresías de grupos del proceso sshd, si la configuración especifica la ejecución del comando como un usuario diferente. Dependiendo de la configuración del sistema, los grupos heredados pueden permitir que los programas auxiliares
CVE-2023-51385	Media	OpenSSH	En SSH en OpenSSH anterior a 9.6, la inyección de comandos del sistema operativo puede ocurrir si un nombre de usuario o nombre de host tiene meta caracteres de Shell, y un token de expansión hace referencia a este nombre en ciertas situaciones.
CVE-2018-15919	Media	OpenSSH	El comportamiento observable de forma remota en auth-gss2.c en OpenSSH hasta 7.8 podría ser utilizado por atacantes remotos para detectar la existencia de usuarios en un sistema objetivo cuando GSS2 está en uso.
CVE-2023-45802	Media	Apache	Servidor HTTP Apache: la memoria de flujo HTTP/2 no se recupera de inmediato en RST: cuando un cliente restablece un flujo HTTP/2 (marco RST), había una ventana de tiempo en la que se realizaba la solicitud. Los recursos de memoria no se recuperaron inmediatamente.
CVE-2021-2389	Media	MySQL	Vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: InnoDB). Las versiones compatibles que se ven afectadas son la 5.7.34 y anteriores y la 8.0.25 y anteriores. Una vulnerabilidad difícil de explotar permite que un atacante no autenticado con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos a esta vulnerabilidad pueden resultar en una capacidad no autorizada de provocar un bloqueo o una falla frecuentemente repetible (DOS completo) del servidor MySQL.
CVE-2018-20685	Media	OpenSSH	En OpenSSH 7.9, scp.c en el cliente scp permite que los servidores SSH omitan las restricciones de acceso planeadas mediante un nombre de archivo "." o un nombre de archivo vacío.
CVE-2019-6109	Media	OpenSSH	Se ha descubierto un problema en OpenSSH 7.9. Debido a la falta de cifrado de caracteres en la pantalla de progreso, un servidor malicioso (o atacante Man-in-the-Middle) puede emplear nombres de objeto manipulados para manipular la salida del cliente.
CVE-2019-6110	Media	OpenSSH	En OpenSSH 7.9, un servidor malicioso (o atacante Man-in-the-Middle) puede manipular la salida del cliente.
CVE-2019-6111	Media	OpenSSH	Se ha descubierto un problema en OpenSSH 7.9. Debido a que la implementación de SCP deriva del rcp 1983, el servidor elige qué archivos/directorios se están enviando al cliente. Sin embargo, el cliente scp solo realiza la validación superficial del nombre de objeto devuelto (solo se evitan los ataques de salto de directorio).
CVE-2021-36368	Baja	OpenSSH	Se ha detectado un problema en OpenSSH versiones anteriores a 8.9. Si un cliente está usando autenticación de clave pública con reenvío de agentes, pero sin -oLogLevel=verbose, y un atacante ha modificado silenciosamente el servidor para que soporte la opción de autenticación None, entonces el usuario no puede determinar si la autenticación FIDO va a confirmar que el usuario desea conectarse a ese servidor.

Tabla 5. Identificación de vulnerabilidades

Al finalizar el proceso, se evidencian los riesgos más importantes a los que está asociado el activo, que al no corregirse se podrán materializar generando un impacto negativo a la universidad.

mero de activo	Nombre del activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad				
				CID	Nivel amenaza	Nivel vulnerabilidad	Controles implementados existentes	Calculo evaluación del riesgo	Nivel de riesgo
R3 - 48	Servidor Linux - Ubuntu Dashboard	Indisponibilidad de servicio	No existe equipo de respaldo	3	2	3	No	18	Alto
		Uso no autorizado del equipo	Escalación de privilegios	2	2	2	No	8	Medio
		Corrupción de datos	No cuenta con sistemas de backups	3	2	3	No	18	Alto
		Mal funcionamiento del software	Sistemas desactualizados	3	2	3	No	18	Alto
		Error en el uso	Configuración incorrecta de parámetros	3	1	2	Soporte contratado con el desarrollador	6	Medio
		Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente	2	2	2	No	8	Medio
		Falla del equipo	Ausencia de planes de continuidad	2	2	2	No	8	Medio

Tabla 6. Nivel de riesgo

3.4. Etapa 4 - Actuar

De acuerdo con la información recolectada en la gestion del riesgo, se encontraron las siguientes fallas y vulnerabilidades:

- No se cuenta con un sistema de alta disponibilidad para fallas eventuales que pueden surgir como interrupción del servicio por causas humanas y daños de hardware.
- No cuenta con una política de backup, en caso de ataques como el rasomware, o corrupción de datos, se deberá implementar desde cero generando inactividad y costos adicionales.

- No cuenta con un plan de mantenimiento preventivo y correctivo documentado.
- El activo no cuenta con una política para el uso no autorizado del equipo.
- Sistema operativo desactualizado, donde los servicios HTTP, SSH, MySQL son los mas débiles.

De las vulnerabilidades presentadas se hacen las siguientes recomendaciones:

- Tener un sistema de replicación en diferente cluster.
- Tener un sistema de respaldo en medios físicos.
- Programar y documentar mantenimientos preventivos y correctivos de manera periodica.
- Acceso de privilegios mínimos, autenticación MFA y configurar reglas locales que permita el acceso solo desde el equipo administrador del activo.
- Realizar actualización del sistema operativo y aplicaciones desde los repositorios oficiales, hacerlos de otros sitios compromete el activo.
- Si no se aplican la actualización del activo de los servicios las cuales tienen vulnerabilidades críticas se deben tomar medidas de mitigación para bloquear peticiones de servidores no o dispositivos no habilitados.
- Actualizar MySQL a la ultima version recomendada por el fabricante
- Cerrar el puerto 3306 y permitir solo peticiones de dispositivos autorizados.
- Actualizar OpenSSH a la última versión recomendada por el fabricante
- Se debe cambiar el puerto de acceso al servidor a 443 puerto seguro.
- Uso de certificados SSL/TLS por una CA de confiaza para verificar la identidad y estblecer una conexión de red segura.

4. Conclusiones y recomendaciones

4.1 Conclusiones

De acuerdo con los resultados obtenidos a través de la normatividad vigente, se demuestra que realizar un análisis y gestión del riesgo es esencial para identificar los controles existentes, las vulnerabilidades o fallas y las amenazas asociadas que pueden causar un daño potencial, además de la identificación previa realizada con el fin de clasificar el activo según la importancia y criticidad del servicio para la universidad. Se encontraron otras vulnerabilidades asociadas que no fueron detectadas en el primer escaneo con la herramienta Nessus, por lo que es recomendable utilizar varias herramientas para ampliar la superficie de ataque.

Con los resultados obtenidos y la metodología del hacking ético, se propuso recomendaciones a partir de las vulnerabilidades encontradas con el fin de aumentar los niveles de seguridad. Recalcar lo importante que puede llegar a ser para la organización el SGSI (sistema de gestión de la seguridad de la información) ya que a través de su enfoque sistemático establece y mejora la postura de seguridad de la información.

Se han implementado algunos controles para proteger el activo, pero no son los suficientes para cubrir en su totalidad el problema de seguridad, al utilizar metodologías como la ISO27001 y las buenas prácticas contempladas benefician de una manera significativa el control y seguimiento de los riesgos.
Es de suma importancia implementar auditorias periódicas, para medir la efectividad de las soluciones implementadas para los riesgos encontrados, estableciendo una cultura de seguridad.

Gracias a las prácticas y enseñanzas proporcionadas por los instructores a lo largo del periodo, se establecieron habilidades necesarias para llevar a cabo en cualquier ámbito, identificando los puntos de falla a los cuales está expuesto cualquier activo de información y que con la ayuda de las diferentes metodologías propuestas a nivel mundial poder garantizar la seguridad de la información.

4.2 Recomendaciones

Se recomienda realizar periódicamente la actualización de los parches de las aplicaciones encontradas OpenSSH, MySQL y Apache a la última versión liberada por el fabricante.

Se recomienda mantener el sistema operativo actualizado y con licencia.

Se recomienda hacer el uso de antivirus, con restricciones para el usuario.

Realizar auditorías de seguridad de forma periódica en los activos de información para identificar posibles puntos débiles y reforzar las medidas de protección.

Promover capacitaciones en seguridad de la información a todo el personal involucrado, para fomentar una cultura de seguridad en la organización.

Se recomienda una política de Backup en caso de presentar un evento inesperado.

Realizar un análisis de riesgos sobre los activos, clasificando el nivel de criticidad en la organización.

Implementar controles a todos los activos sin importar el nivel de criticidad para la organización, por mínima que sea la brecha de seguridad puede generar un punto de acceso no autorizado a la información causando un impacto negativo.

Desarrollar reglas de administración desde el activo, asegurando que solo se tenga el acceso a su gestión desde los equipos permitidos, políticas de descarga y ejecución de archivos.

Una vez aplicada las acciones de mejora y promover de manera continua la seguridad de la información, se recomienda realizar nuevamente el proceso de evaluación para mitigar o eliminar el riesgo.

Si la organización cuenta con una zona de seguridad realizar el paso de este servidor a esta zona lo cual permitirá tener el control de acceso y verificación del flujo del tráfico hacia al servidor.

5. Anexos

Anexo A: Análisis y gestión del riesgo.

Bibliografía

Bases de datos. Vulnerabilidades Comunes Existentes. CVE-details disponible: [en línea]. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. Retrieved May 22, 2024, from https://www.cvedetails.com/

Ciberseguridad. SOPHOS. Maya Horowitz. análisis global. (2024). Global analysis. https://go.checkpoint.com/2024-cyber-security-report/chapter-04.php

ISO 27001. España: ISO 27001. Controles ISO 27002 punto por punto disponible:[en línea]. (n.d.). SGSI. Retrieved May 22, 2024, from https://www.iso27000.es/

Ministerio de Tecnologías de la Información y las Comunicaciones. Guía De Gestión De Riesgos. Seguridad Y Privacidad De La Información. [en línea] disponible: [en línea]: (2020). Guía de gestión de riesgos. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

NIST. NATIONAL VULNERABILITY DATABASE [En línea] disponible en: (n.d.). NVD - Vulnerabilities. Retrieved May 22, 2024, from https://nvd.nist.gov/vuln

Ciberseguridad, S. News. E. E. del R. en el S. Educativo. [en línea] disponible en: (2023). sophos-state-of-ransomware-education-2023-wpes.

Ec Council, CEH Ethical Hacking and Countermeasures v11. 2020.

Veloz, J., Alcívar, A., Salvatierra, G., & Silva, C. Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta KALI-LINUX.

Instituto Nacional de Ciberseguridad. Incibe disponible: [en línea] https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/