Análisis Forense y Fortalecimiento de Infraestructura Crítica

Proyecto: Proyecto Final de Ciberseguridad.

Fecha de Ejecución: Febrero 2026

Elaborado por: Jose Rodriguez

Introducción al proyecto

El Objetivo es Transformar un activo vulnerable en un entorno seguro bajo estándares profesionales

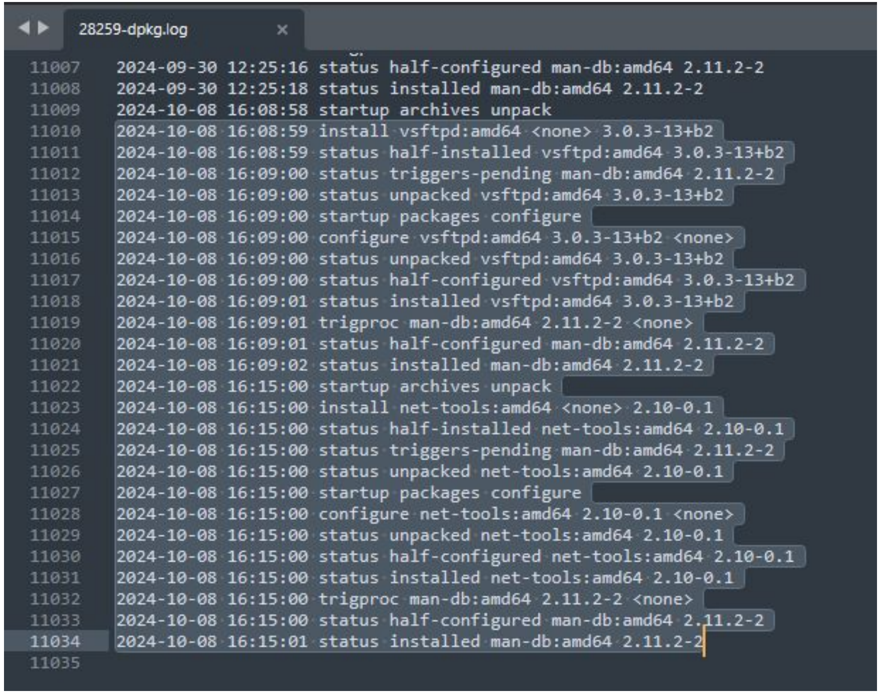
Se buscó identificar cómo entraron los atacantes, sacarlos y asegurarse de que no puedan volver a ingresar

Alcance

- Investigación de "huellas digitales" (Análisis Forense)
- Simulación de ataques controlados (Auditoría Ofensiva)
- Reparación y blindaje (Remediación)
- Reglas y manuales de protección (Gobernanza)

Hallazgos

- Acceso por fuerza bruta
- Instalación de herramientas intrusas
- Manipulación de la web
- Persistencia
- Borrado de huellas



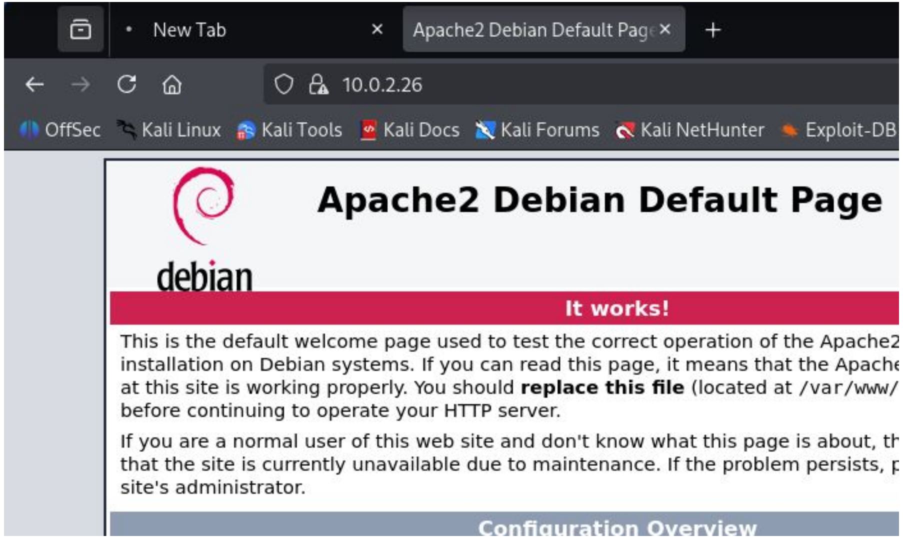
```
2024-09-30 12:25:16 status half-configured man-db:amd64 2.11.2-2
2024-09-30 12:25:18 status installed man-db:amd64 2.11.2-2
2024-10-08 16:08:58 startup archives unpack
2024-10-08 16:08:59 install vsftpd:amd64 <none> 3.0.3-13+b2
2024-10-08 16:08:59 status half-installed vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 status triggers-pending man-db:amd64 2.11.2-2
2024-10-08 16:09:00 status unpacked vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 startup packages configure
2024-10-08 16:09:00 configure vsftpd:amd64 3.0.3-13+b2 <none>
2024-10-08 16:09:00 status unpacked vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 status half-configured vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:01 status installed vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:01 trigproc man-db:amd64 2.11.2-2 <none>
2024-10-08 16:09:01 status half-configured man-db:amd64 2.11.2-2
2024-10-08 16:09:02 status installed man-db:amd64 2.11.2-2
2024-10-08 16:15:00 startup archives unpack
2024-10-08 16:15:00 install net-tools:amd64 <none> 2.10-0.1
2024-10-08 16:15:00 status half-installed net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status triggers-pending man-db:amd64 2.11.2-2
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 startup packages configure
2024-10-08 16:15:00 configure net-tools:amd64 2.10-0.1 <none>
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status half-configured net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status installed net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 trigproc man-db:amd64 2.11.2-2 <none>
2024-10-08 16:15:00 status half-configured man-db:amd64 2.11.2-2
2024-10-08 16:15:01 status installed man-db:amd64 2.11.2-2
```

Impacto

Toma de control absoluto

Acceso a información sensible

Pérdida de acceso a los Servicios



Apache2 Debian Default Page

It works!

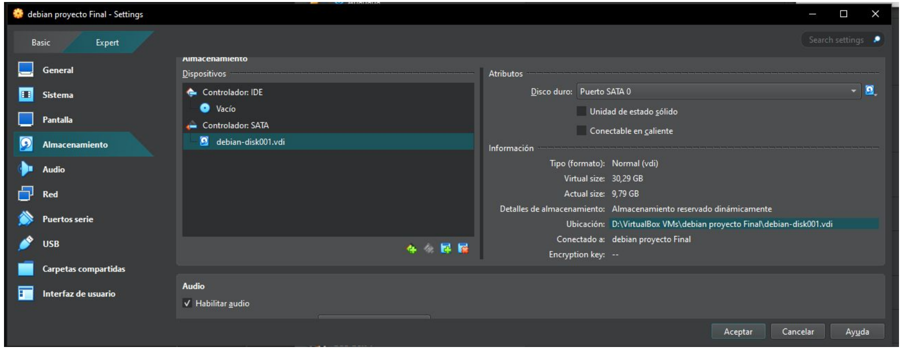
This is the default welcome page used to test the correct operation of the Apache2 installation on Debian systems. If you can read this page, it means that the Apache at this site is working properly. You should **replace this file** (located at /var/www/ before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, th that the site is currently unavailable due to maintenance. If the problem persists, p site's administrator.

Configuration Overview

Análisis Forense

- Preservación de la evidencia
- Herramientas especializadas
- Analisis sobre Copia Bit a Bit



Almacenamiento

Dispositivos

- Controlador: IDE
  - Vacío
- Controlador: SATA
  - debian-disk001.vdi

Atributos

Disco duro: Puerto SATA 0

□ Unidad de estado sólido

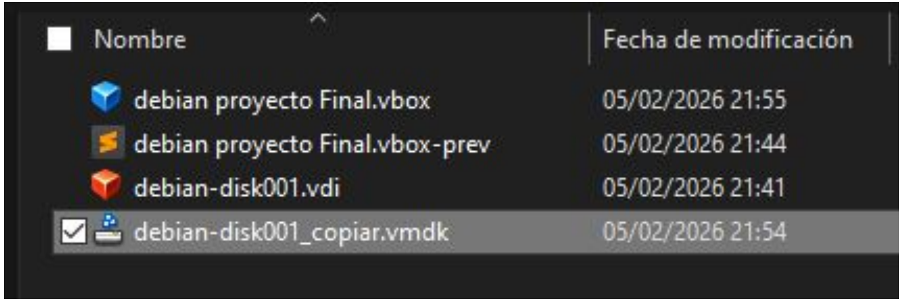
□ Conectable en caliente

Información

Tipo (formato):	Normal (vdi)
Virtual size:	30,29 GB
Actual size:	9,79 GB
Detalles de almacenamiento:	Almacenamiento reservado dinámicamente
Ubicación:	D:\VirtualBox VMs\debian proyecto Final\debian-disk001.vdi
Conectado a:	debian proyecto Final
Encryption key:	--

Audio

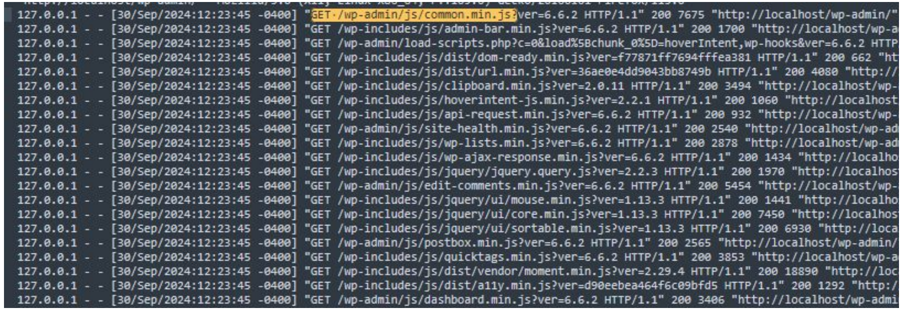
☑ Habilitar audio



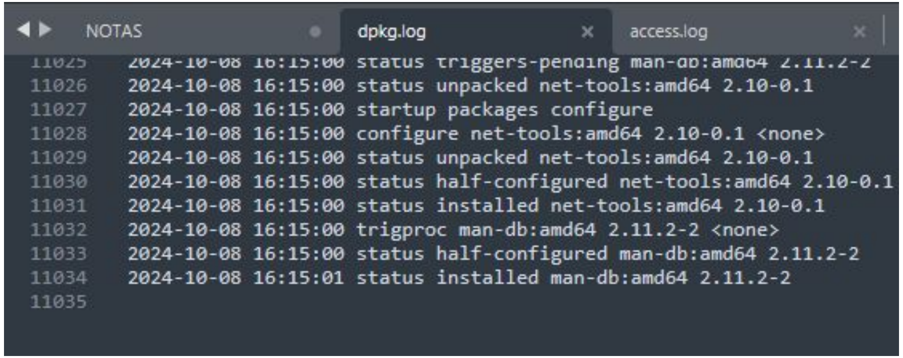
□ Nombre	Fecha de modificación
debian proyecto Final.vbox	05/02/2026 21:55
debian proyecto Final.vbox-prev	05/02/2026 21:44
debian-disk001.vdi	05/02/2026 21:41
☑ debian-disk001_copiar.vmdk	05/02/2026 21:54

Linea de Tiempo

- **01 octubre 2024**
  - 01:06 - Reconocimiento Automatizado
- **08 de Octubre 2024**
  - 21:50 - Ataque de Diccionario
  - 22:05 - Primer acceso
  - 22:49 - Acceso al Panel Administrativo del Wordpress
  - 22:58 - Limpieza de huellas



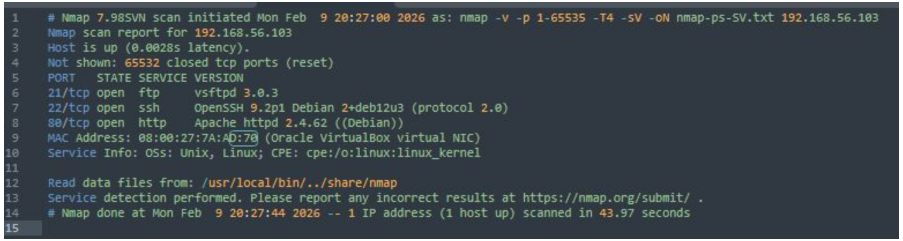
```
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/js/common.min.js?ver=6.6.2 HTTP/1.1" 200 7675 "http://localhost/wp-admin/"
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/admin-bar.min.js?ver=6.6.2 HTTP/1.1" 200 1700 "http://localhost/wp-a
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/load-scripts.php?c=0&load%5Bchunk_0%5D=hoverIntent,wp-hooks&ver=6.6.2 HTTP
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/dist/dom-ready.min.js?ver=f77871ff7694fffea381 HTTP/1.1" 200 662 "ht
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/dist/url.min.js?ver=36ae0e4dd9043bb8749b HTTP/1.1" 200 4080 "http://
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/clipboard.min.js?ver=2.0.11 HTTP/1.1" 200 3494 "http://localhost/wp-
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/hoverintent-js.min.js?ver=2.2.1 HTTP/1.1" 200 1060 "http://localhost
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/api-request.min.js?ver=6.6.2 HTTP/1.1" 200 932 "http://localhost/wp-
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/js/site-health.min.js?ver=6.6.2 HTTP/1.1" 200 2540 "http://localhost/wp-ad
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/wp-lists.min.js?ver=6.6.2 HTTP/1.1" 200 2878 "http://localhost/wp-ad
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/wp-ajax-response.min.js?ver=6.6.2 HTTP/1.1" 200 1434 "http://localho
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/jquery/jquery.query.js?ver=2.2.3 HTTP/1.1" 200 1970 "http://localhos
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/js/edit-comments.min.js?ver=6.6.2 HTTP/1.1" 200 5454 "http://localhost/wp-
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/jquery/ui/mouse.min.js?ver=1.13.3 HTTP/1.1" 200 1441 "http://localho
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/jquery/ui/core.min.js?ver=1.13.3 HTTP/1.1" 200 7450 "http://localhos
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/jquery/ui/sortable.min.js?ver=1.13.3 HTTP/1.1" 200 6930 "http://loca
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/js/postbox.min.js?ver=6.6.2 HTTP/1.1" 200 2565 "http://localhost/wp-admin/
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/quicktags.min.js?ver=6.6.2 HTTP/1.1" 200 3853 "http://localhost/wp-a
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/dist/vendor/moment.min.js?ver=2.29.4 HTTP/1.1" 200 18890 "http://loc
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-includes/js/dist/a11y.min.js?ver=d90eebea464f6c09bfd5 HTTP/1.1" 200 1292 "http:/
127.0.0.1 - - [30/Sep/2024:12:23:45 -0400] "GET /wp-admin/js/dashboard.min.js?ver=6.6.2 HTTP/1.1" 200 3406 "http://localhost/wp-admi
```



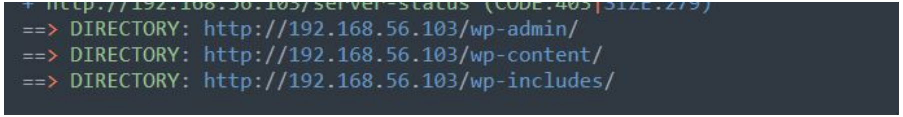
```
2024-10-08 16:15:00 status triggers-pending man-db:amd64 2.11.2-2
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 startup packages configure
2024-10-08 16:15:00 configure net-tools:amd64 2.10-0.1 <none>
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status half-configured net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status installed net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 trigproc man-db:amd64 2.11.2-2 <none>
2024-10-08 16:15:00 status half-configured man-db:amd64 2.11.2-2
2024-10-08 16:15:01 status installed man-db:amd64 2.11.2-2
```

Auditoría Ofensiva

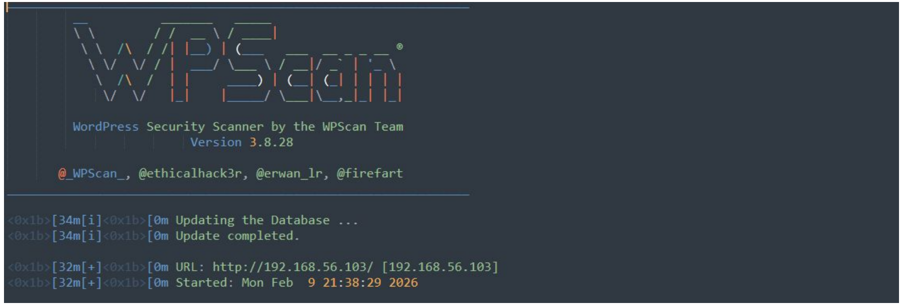
- Identificacion
- Escaneo de posibles vulnerabilidades
- Simulación de ataques
- Confirmación de vulnerabilidades



```
# Nmap 7.98SVN scan initiated Mon Feb  9 20:27:00 2026 as: nmap -v -p 1-65535 -T4 -sV -oN nmap-ps-SV.txt 192.168.56.103
Nmap scan report for 192.168.56.103
Host is up (0.0028s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:7A:AD:70 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Feb  9 20:27:44 2026 -- 1 IP address (1 host up) scanned in 43.97 seconds
```



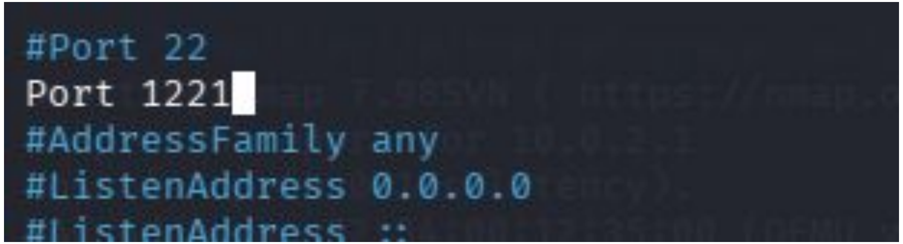
```
+ http://192.168.56.103/server-status (CODE:403|SIZE:279)
==> DIRECTORY: http://192.168.56.103/wp-admin/
==> DIRECTORY: http://192.168.56.103/wp-content/
==> DIRECTORY: http://192.168.56.103/wp-includes/
```



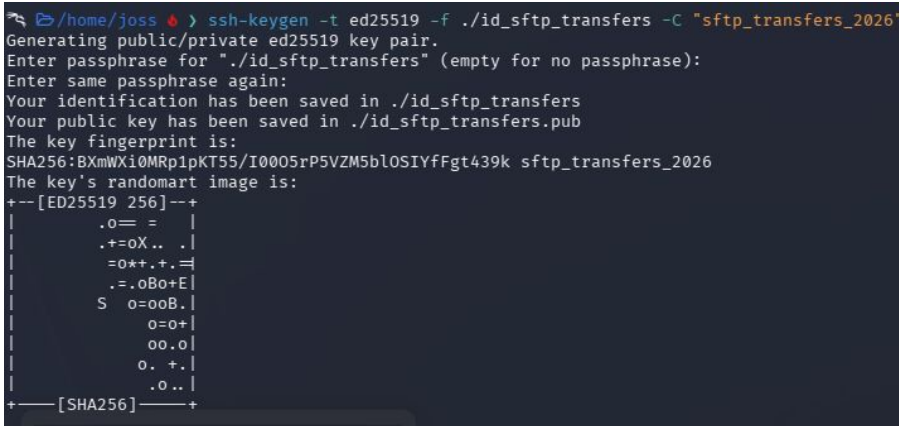
```
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

<0x1b>[34m[i]<0x1b>[0m Updating the Database ...
<0x1b>[34m[i]<0x1b>[0m Update completed.

<0x1b>[32m[+]<0x1b>[0m URL: http://192.168.56.103/ [192.168.56.103]
<0x1b>[32m[+]<0x1b>[0m Started: Mon Feb  9 21:38:29 2026
```

Fortalecimiento de Accesos

- Cierre de accesos innecesarios
  - Puerto 21
  - Puerto 80
- Nuevas cerraduras
  - Cambio puerto común
  - Llaves Digitales
  - Cifrado WEB
  - Nuevas Credenciales



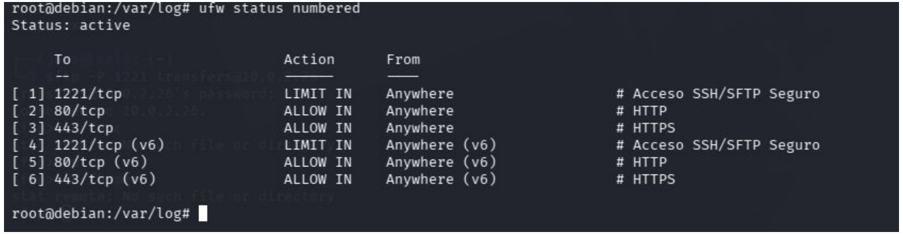
```
#Port 22
Port 1221
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```



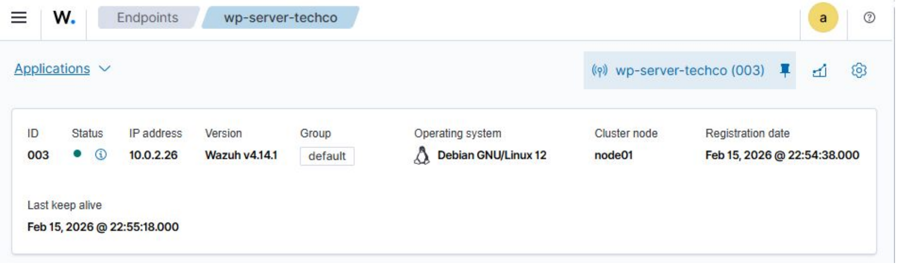
```
/home/joss ❯ ssh-keygen -t ed25519 -f ./id_sftp_transfers -C "sftp_transfers_2026"
Generating public/private ed25519 key pair.
Enter passphrase for "./id_sftp_transfers" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./id_sftp_transfers
Your public key has been saved in ./id_sftp_transfers.pub
The key fingerprint is:
SHA256:BXmWXi0MRp1pKT55/I00O5rP5VZM5blOSIYfFgt439k sftp_transfers_2026
The key's randomart image is:
+--[ED25519 256]--+
|        .o== =   |
|        .+=oX.. .|
|         =o*+.+.=|
|         .=.oBo+E|
|        S  o=ooB.|
|             o=o+|
|             oo.o|
|            o. +.|
|             .o..|
+----[SHA256]-----+
```

Barreras y Monitoreo Activo

- Muro de protección (Firewall)
- Bloqueos automaticos a ataques
- Vigilancia automática



```
root@debian:/var/log# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 1221/tcp                   LIMIT IN    Anywhere                   # Acceso SSH/SFTP Seguro
[ 2] 80/tcp                     ALLOW IN    Anywhere                   # HTTP
[ 3] 443/tcp                    ALLOW IN    Anywhere                   # HTTPS
[ 4] 1221/tcp (v6)              LIMIT IN    Anywhere (v6)              # Acceso SSH/SFTP Seguro
[ 5] 80/tcp (v6)                ALLOW IN    Anywhere (v6)              # HTTP
[ 6] 443/tcp (v6)               ALLOW IN    Anywhere (v6)              # HTTPS

root@debian:/var/log# 
```



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date
003	●	10.0.2.26	Wazuh v4.14.1	default	Debian GNU/Linux 12	node01	Feb 15, 2026 @ 22:54:38.000

Last keep alive
Feb 15, 2026 @ 22:55:18.000

Cumplimiento Normativo y Gobernanza

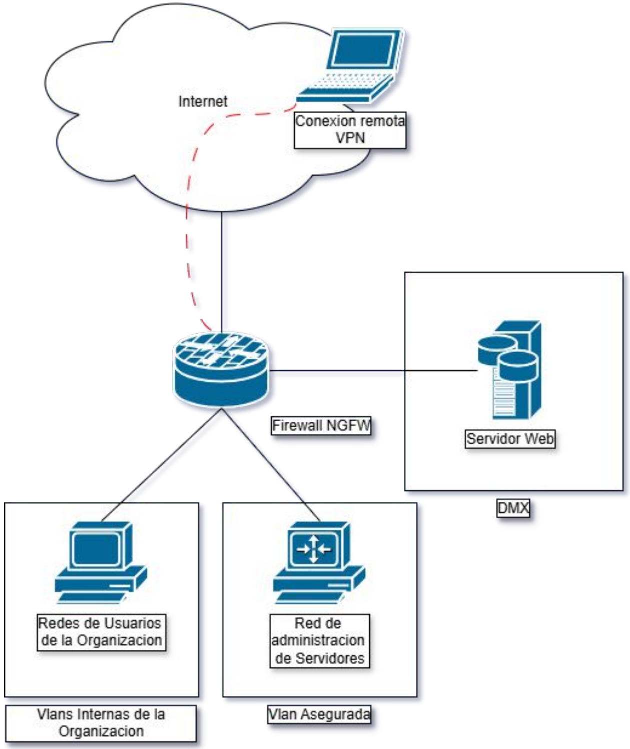
- Importancia del Cumplimiento Normativo
- Plan de respuesta
- Protección de datos
- Gestión de riesgos

ISO
27001

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Conclusiones

- Transformación integral del servidor.
- Implementación de una estrategia de defensa en profundidad.
- Integración de herramientas de monitoreo proactivo.
- Respuesta automatizada ante incidentes.
- Sistema de Gestión de Seguridad de la Información


Internet
Conexion remota VPN
Firewall NGFW
Servidor Web
DMX
Redes de Usuarios de la Organizacion
Red de administracion de Servidores
Vlans Internas de la Organizacion
Vlan Asegurada