TechCorp Inc.

INFORME DE INCIDENTE DE SEGURIDAD

SERVIDOR: **DEBIAN-FINAL-PROJECT**

2 de mayo 2025

Departamento de Seguridad de la Información
Tech Corp inc

1. RESUMEN EJECUTIVO

- **Fecha del incidente**: 08/10/202
- **Tipo de incidente**: Acceso remoto no autorizado con privilegios de root
- **Impacto:** Compromiso total del sistema, exposición de servicios críticos y posible persistencia maliciosa.
- **Servicios involucrados:** SSH, Apache2, vsftpd, MariaD
- **Estado actual:** Incidente contenido y mitigado.
- **Medidas ejecutadas:**
    - Bloqueo de acceso root por SSH.
    - Cierre de FTP.
    - Revisión y aseguramiento del servidor web.
    - Restauración de permisos y verificación de servicios.

- **Recomendaciones clave:**
    - Realizar Penstesting
    - Aplicar hardening del sistema operativo
    - Implementar monitoreo activo (Wazuh)
    - Prohibir accesos root directos por SSH.
    - Aplicar control de integridad y políticas de mínimos privilegios.

2. IDENTIFICACION DEL INCIDENTE

- **Nombre de quien reporta:** Yorman Velo
- **Cargo:** Analista de Seguridad e la Información
- **Correo electrónico:** yveloz@techcorp.co
- **Fecha de identificación:** 02/05/2025
- **Descripción del Incidente:** Durante una auditoría de seguridad en una máquina Debian provista como entorno de laboratorio, se detectó un acceso remoto no autorizado a través del servicio SSH, utilizando la cuenta root. El atacante obtuvo acceso privilegiado desde la dirección **IP 192.168.0.134,** y aprovechó el entorno expuesto para interactuar con servicios como Apache2, FTP y MariaDB, todos activos al momento del análisis.

3. ANALISIS DEL INCIDENTE

- **Fecha de Inicio del Incidente:** 08/10/2024 a las 17:40:59 horas.
- **Fecha de finalización del Incidente:** 08/10/2024 (presunto), posterior a las 18:00 horas.
- **Clasificación del Incidente:**
    - Acceso no autorizado
    - Compromiso de cuenta de usuario privilegiada
    - Manipulación de la Configuración
    - Compromiso de la integridad de servicio
    - Posible persistencia (webshell / FTP)
    - Riesgo de alteración de datos

- **Impacto:** CRITICO
- **Descripción completa del análisis:** Mediante **sudo journalctl -u ssh**, se detectó un acceso exitoso como root desde una IP externa. Simultáneamente, se verificó la exposición de servicios:
    - Apache HTTP (puerto 80)
    - FTP (vsftpd, puerto 21)
    - MariaDB (puerto 3306)

En /var/www/html se encontraron múltiples archivos de una instalación de WordPress, todos con permisos **-rwxrwxrwx (777)**, lo cual representa un riesgo extremo de ejecución arbitraria. No se evidenció actividad directa en crontab, pero se identificaron servicios como rsync y rc-local que podrían permitir persistencia si configurados.

Adicionalmente, no se encontraron servicios de auditoría como **auditd** o **rsyslog**, lo cual puede indicar una acción deliberada para eliminar registros y ocultar actividad.

- Causas:
    - Configuración insegura de SSH: Permitía login directo con usuario root.
    - Falta de políticas de hardening: Permisos 777, servicios innecesarios habilitados (FTP).
    - Servicios innecesarios expuestos sin monitoreo.
    - Ausencia de controles de auditoría y detección temprana.

- Sistemas Afectados:
    - Debian GNU/Linux (entorno completo)
    - Apache2
    - Vsftpd
    - MariaDB

- Acciones de contención:
    - Snapshot del sistema para análisis posterior
    - Verificación y aislamiento de la sesión root sospechosa
    - Detención de servicios FTP y desactivación de root por SSH
    - Extracción de evidencia desde logs, crontab y servicio

- Acciones de correctivas y de contención:

    - **Snapshot del sistema para análisis posterior**

    - **Desactivación de vsftpd, avahi-daemon, cups**
      sudo systemctl disable vsftpd --now
      sudo systemctl disable cups --now
      sudo systemctl disable avahi-daemon --now

    - **Cambios de contraseña usuario root**
      Passwd root

    - **Modificación de /etc/ssh/sshd_config para prohibir root login**
      sudo nano /etc/ssh/sshd_config
      # Cambiar:
      PermitRootLogin no

    - **Cambios de permisos en /var/www/html**
      sudo find /var/www/html -type f -exec chmod 644 {} \;
      sudo find /var/www/html -type d -exec chmod 755 {} \;

    - **Aplicación de parches y actualizaciones del sistema**
      sudo apt update && sudo apt upgrade –y

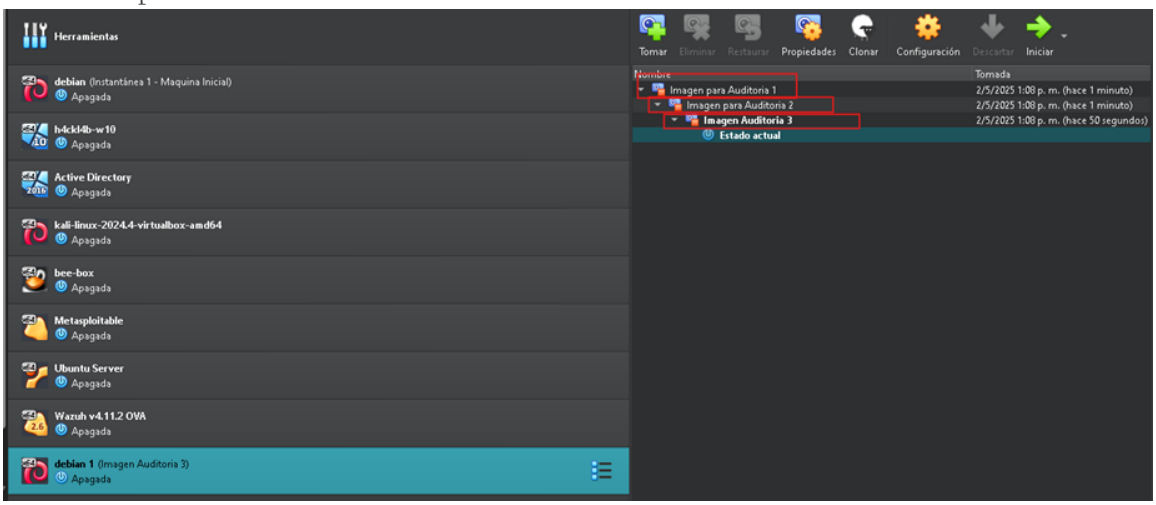
    - **Instalación de wazuh- Agent**

4. CIERRE DEL INCIDENTE

- **Fue solucionado el incidente:** Si
- **Efectividad de las acciones correctivas: Alta**. Se eliminaron los servicios vulnerables, se bloquearon entradas inseguras, y se corrigieron configuraciones críticas.
- **Lecciones aprendidas:**
    - Las configuraciones por defecto de servicios como SSH y FTP representan riesgos si no se revisan.
    - La exposición de servidores web debe estar acompañada de monitoreo activo.
    - Es crítica la presencia de servicios de auditoría (auditd, rsyslog) para la detección temprana y trazabilidad.
    - Nunca se deben asignar permisos 777 a archivos accesibles por red.
    - Todo entorno con acceso root debe estar controlado y monitoreado.

5. ANEXO I – EVIDENCIA TECNICA

- Snapshots del sistema



- Acceso root por SSH: **sudo journalctl -u ssh**

```
File  Edit  View  Search  Terminal  Help
Oct 08 16:48:02 debian sshd[555]: Server listening on 0.0.0.0 port 22.
Oct 08 16:48:02 debian sshd[555]: Server listening on :: port 22.
Oct 08 16:48:02 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot af0a79f76920440c8e08594d6547449b --
Oct 08 17:28:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 08 17:28:38 debian sshd[550]: Server listening on 0.0.0.0 port 22.
Oct 08 17:28:38 debian sshd[550]: Server listening on :: port 22.
Oct 08 17:28:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
-- Boot 531a5025512a4ec2855bf7b4e3629dab --
May 02 11:50:37 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 02 11:50:38 debian sshd[582]: Server listening on 0.0.0.0 port 22.
May 02 11:50:38 debian sshd[582]: Server listening on :: port 22.
May 02 11:50:38 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
May 02 12:00:37 debian systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
May 02 12:00:37 debian sshd[582]: Received signal 15; terminating.
May 02 12:00:37 debian systemd[1]: ssh.service: Deactivated successfully.
May 02 12:00:37 debian systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
-- Boot 5feded3ce9704a72900c5e61b170f1a5 --
May 02 12:13:03 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 02 12:13:04 debian sshd[578]: Server listening on 0.0.0.0 port 22.
May 02 12:13:04 debian sshd[578]: Server listening on :: port 22.
```

- Permisos 777 en WordPress: **ls -la /var/www/html/**

```
debian@debian:~$ ls -la /var/www/html/
total 256
drwxrwxrwx  5 www-data www-data  4096 Oct  8  2024 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rwxrwxrwx  1 www-data www-data   523 Sep 30  2024 .htaccess
-rwxrwxrwx  1 www-data www-data 10701 Sep 30  2024 index.html
-rwxrwxrwx  1 www-data www-data   405 Feb  6  2020 index.php
-rwxrwxrwx  1 www-data www-data 19915 Dec 31  2023 license.txt
-rwxrwxrwx  1 www-data www-data  7409 Jun 18  2024 readme.html
-rwxrwxrwx  1 www-data www-data  7387 Feb 13  2024 wp-activate.php
drwxrwxrwx  9 www-data www-data  4096 Sep 10  2024 wp-admin
-rwxrwxrwx  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rwxrwxrwx  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rwxrwxrwx  1 www-data www-data  3017 Sep 30  2024 wp-config.php
drwxrwxrwx  5 www-data www-data  4096 Oct  8  2024 wp-content
-rwxrwxrwx  1 www-data www-data  5638 May 30  2023 wp-cron.php
drwxrwxrwx 30 www-data www-data 12288 Sep 10  2024 wp-includes
-rwxrwxrwx  1 www-data www-data  2502 Nov 26  2022 wp-links-opml.php
-rwxrwxrwx  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rwxrwxrwx  1 www-data www-data 51238 May 28  2024 wp-login.php
-rwxrwxrwx  1 www-data www-data  8525 Sep 16  2023 wp-mail.php
-rwxrwxrwx  1 www-data www-data 28774 Jul  9  2024 wp-settings.php
-rwxrwxrwx  1 www-data www-data 34385 Jun 19  2023 wp-signup.php
-rwxrwxrwx  1 www-data www-data  4885 Jun 22  2023 wp-trackback.php
-rwxrwxrwx  1 www-data www-data  3246 Mar  2  2024 xmlrpc.php
debian@debian:~$
```

- FTP activo: **systemctl status vsftpd**

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-02 14:57:49 EDT; 5h 0min ago
    Process: 530 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 537 (vsftpd)
      Tasks: 1 (limit: 2284)
     Memory: 1.0M
        CPU: 19ms
     CGroup: /system.slice/vsftpd.service
             └─537 /usr/sbin/vsftpd /etc/vsftpd.conf

Warning: some journal files were not opened due to insufficient permissions.
debian@debian:~$
```

- Base de datos activa: **systemctl status mariadb**

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ systemctl status mariadb
● mariadb.service - MariaDB 10.11.6 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-02 14:57:53 EDT; 5h 2min ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 525 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
    Process: 542 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 553 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`cd /usr/bin/..; /usr/bin/galera_
    Process: 693 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 697 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 643 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 8 (limit: 2284)
     Memory: 250.0M
        CPU: 8.811s
     CGroup: /system.slice/mariadb.service
             └─643 /usr/sbin/mariadbd

Warning: some journal files were not opened due to insufficient permissions.
lines 1-19/19 (END)
```

```
debian@debian:~$ sudo grep -R "bind-address" /etc/mysql/
/etc/mysql/mariadb.conf.d/50-server.cnf:bind-address            = 127.0.0.1
/etc/mysql/mariadb.conf.d/60-galera.cnf:#bind-address = 0.0.0.0
```

- Ausencia de auditd y rsyslog : **cat /var/log/auth.log** y **cat /var/log/syslog**

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ cat /var/log/auth.log
cat: /var/log/auth.log: No such file or directory
debian@debian:~$ cat /var/log/syslog
cat: /var/log/syslog: No such file or directory
debian@debian:~$
```

- Cronjobs: **Sudo cat /etc/crontab**

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6    * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6    1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
```

6. ANEXO I – ACCIONES CORRECTIVAS

Acción correctiva 1:

```
debian@debian:~$ sudo systemctl disable vsftpd --now
[sudo] password for debian:
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".
debian@debian:~$ sudo systemctl status  vsftpd
○ vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: enabled)
     Active: inactive (dead)

May 06 18:00:13 debian systemd[1]: Starting vsftpd.service - vsftpd FTP server...
May 06 18:00:13 debian systemd[1]: Started vsftpd.service - vsftpd FTP server.
May 06 20:19:55 debian systemd[1]: Stopping vsftpd.service - vsftpd FTP server...
May 06 20:19:55 debian systemd[1]: vsftpd.service: Deactivated successfully.
May 06 20:19:55 debian systemd[1]: Stopped vsftpd.service - vsftpd FTP server.
debian@debian:~$
```

Acción correctiva 2:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo systemctl disable cups --now
Synchronizing state of cups.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
Removed "/etc/systemd/system/sockets.target.wants/cups.socket".
Removed "/etc/systemd/system/multi-user.target.wants/cups.path".
Removed "/etc/systemd/system/multi-user.target.wants/cups.service".
Removed "/etc/systemd/system/printer.target.wants/cups.service".
debian@debian:~$ sudo systemctl status  cups
○ cups.service - CUPS Scheduler
     Loaded: loaded (/lib/systemd/system/cups.service; disabled; preset: enabled)
     Active: inactive (dead) since Tue 2025-05-06 20:23:58 EDT; 11s ago
   Duration: 2h 23min 41.211s
TriggeredBy: ○ cups.socket
       Docs: man:cupsd(8)
    Process: 754 ExecStart=/usr/sbin/cupsd -l (code=exited, status=0/SUCCESS)
   Main PID: 754 (code=exited, status=0/SUCCESS)
     Status: "Scheduler is running..."
        CPU: 48ms

May 06 18:00:17 debian systemd[1]: Starting cups.service - CUPS Scheduler...
May 06 18:00:17 debian systemd[1]: Started cups.service - CUPS Scheduler.
May 06 20:23:58 debian systemd[1]: Stopping cups.service - CUPS Scheduler...
May 06 20:23:58 debian systemd[1]: cups.service: Deactivated successfully.
May 06 20:23:58 debian systemd[1]: Stopped cups.service - CUPS Scheduler.
debian@debian:~$
```

Acción correctiva 3:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo systemctl disable avahi-daemon --now
Removed "/etc/systemd/system/sockets.target.wants/avahi-daemon.socket".
Removed "/etc/systemd/system/multi-user.target.wants/avahi-daemon.service".
Removed "/etc/systemd/system/dbus-org.freedesktop.Avahi.service".
Warning: Stopping avahi-daemon.service, but it can still be activated by:
  avahi-daemon.socket
debian@debian:~$ sudo systemctl status avahi-daemon
○ avahi-daemon.service - Avahi mDNS/DNS-SD Stack
     Loaded: loaded (/lib/systemd/system/avahi-daemon.service; disabled; preset: enabled)
     Active: inactive (dead) since Tue 2025-05-06 20:28:32 EDT; 23s ago
   Duration: 2h 28min 19.942s
TriggeredBy: • avahi-daemon.socket
    Process: 384 ExecStart=/usr/sbin/avahi-daemon -s (code=exited, status=0/SUCCESS)
   Main PID: 384 (code=exited, status=0/SUCCESS)
     Status: "avahi-daemon 0.8 starting up."
        CPU: 174ms
```

Acción correctiva 4:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
debian@debian:~$ date
Tue May  6 08:40:41 PM EDT 2025
debian@debian:~$
```

Acción correctiva 5:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo nano /etc/ssh/sshd_config
debian@debian:~$ sudo cat /etc/ssh/sshd_config

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

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

# The strategy used for options in the default sshd_config shipped with
# 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.d/*.conf

#Port 22
#AddressFamily any
#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
#MaxSessions 10
```

Acción correctiva 6:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo find /var/www/html/ -type f -exec chmod 644 {} \;
[sudo] password for debian:
debian@debian:~$ sudo find /var/www/html/ -type d -exec chmod 755 {} \;
debian@debian:~$ ls -la /var/www/html/
total 260
drwxr-xr-x  5 www-data www-data  4096 May  6 18:31 .
drwxr-xr-x  3 root     root      4096 Sep 30  2024 ..
-rw-r--r--  1 www-data www-data   523 Sep 30  2024 .htaccess
-rw-r--r--  1 www-data www-data 10701 Sep 30  2024 index.html
-rw-r--r--  1 www-data www-data   405 Feb  6  2020 index.php
-rw-r--r--  1 www-data www-data 19903 May  6 18:31 license.txt
-rw-r--r--  1 www-data www-data  7425 May  6 18:31 readme.html
-rw-r--r--  1 www-data www-data  7387 Feb 13  2024 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 Sep 10  2024 wp-admin
-rw-r--r--  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rw-r--r--  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rw-r--r--  1 www-data www-data  3017 Sep 30  2024 wp-config.php
-rw-r--r--  1 www-data www-data  3336 May  6 18:31 wp-config-sample.php
drwxr-xr-x  6 www-data www-data  4096 May  6 20:49 wp-content
-rw-r--r--  1 www-data www-data  5617 May  6 18:31 wp-cron.php
drwxr-xr-x 30 www-data www-data 12288 May  6 18:31 wp-includes
-rw-r--r--  1 www-data www-data  2502 Nov 26  2022 wp-links-opml.php
-rw-r--r--  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rw-r--r--  1 www-data www-data 51414 May  6 18:31 wp-login.php
-rw-r--r--  1 www-data www-data  8727 May  6 18:31 wp-mail.php
-rw-r--r--  1 www-data www-data 30081 May  6 18:31 wp-settings.php
-rw-r--r--  1 www-data www-data 34516 May  6 18:31 wp-signup.php
-rw-r--r--  1 www-data www-data  5102 May  6 18:31 wp-trackback.php
-rw-r--r--  1 www-data www-data  3205 May  6 18:31 xmlrpc.php
debian@debian:~$
```

Acción correctiva 7:

```
debian@debian:~$ sudo apt-get update
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
debian@debian:~$ date
Tue May  6 09:17:51 PM EDT 2025
debian@debian:~$
```

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ sudo apt-get upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libdaxctl1 libndctl6 libpmem1 linux-image-6.1.0-22-amd64
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  linux-image-amd64
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
debian@debian:~$ date
Tue May  6 09:27:13 PM EDT 2025
debian@debian:~$
```

Acción correctiva 8:

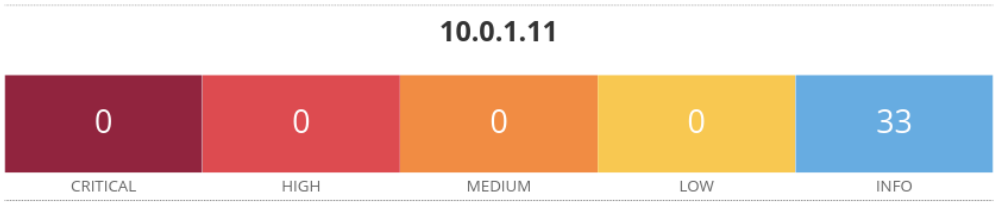
```
debian@debian:~/Downloads$ sudo dpkg -i wazuh-indexer_4.11.2-1_amd64.deb
Selecting previously unselected package wazuh-indexer.
(Reading database ... 170696 files and directories currently installed.)
Preparing to unpack wazuh-indexer_4.11.2-1_amd64.deb ...
Running Wazuh Indexer Pre-Installation Script
Unpacking wazuh-indexer (4.11.2-1) ...
Setting up wazuh-indexer (4.11.2-1) ...
Running Wazuh Indexer Post-Installation Script
### NOT starting on installation, please execute the following statements to configure wazuh-indexer service to sta
utomatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable wazuh-indexer.service
### You can start wazuh-indexer service by executing
 sudo systemctl start wazuh-indexer.service
debian@debian:~/Downloads$
```

Acción correctiva 9:

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb &
& sudo WAZUH_MANAGER='10.0.1.10' WAZUH_AGENT_NAME='newagent' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
--2025-05-07 20:15:22--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.de
b
Resolving packages.wazuh.com (packages.wazuh.com)... 3.160.107.79, 3.160.107.82, 3.160.107.104, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|3.160.107.79|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11075686 (11M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.11.2-1_amd64.deb'

wazuh-agent_4.11.2- 100%[==================>]  10.56M  14.5MB/s    in 0.7s

2025-05-07 20:15:23 (14.5 MB/s) - 'wazuh-agent_4.11.2-1_amd64.deb' saved [11075686/11075686]

[sudo] password for debian:
Selecting previously unselected package wazuh-agent.
(Reading database ... 171876 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.11.2-1_amd64.deb ...
Unpacking wazuh-agent (4.11.2-1) ...
Setting up wazuh-agent (4.11.2-1) ...
debian@debian:~$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent
.service.
debian@debian:~$
```

Acción correctiva 10:

Escaneos de Vulnerabilidades con nessus donde hay evidencia no tener vulnerabilidades.



Vulnerabilities Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)