Fecha: 08 de febrero de 2026
Analista Responsable: Sergio Maturana
Estado: RESUELTO (Cerrado)

INFORME TÉCNICO DE INCIDENTE DE SEGURIDAD

Auditoría, Limpieza y Hardening de Servidor Linux

Sergio Maturana Mena

1 RESUMEN EJECUTIVO

En cumplimiento con los objetivos de la Fase 1, se ha realizado la restauración y protección de un servidor crítico comprometido. Se identificó acceso no autorizado a nivel de root, se contuvo la amenaza, y se aplicaron correcciones de seguridad basadas en estándares de la industria para prevenir la escalación y recurrencia.

2 IDENTIFICACIÓN Y ANÁLISIS FORENSE

2.1 Servicios Comprometidos y Vector de Acceso

Se realizó una auditoría de los registros del sistema (journalctl y logs de autenticación). Se determinó que el atacante comprometió el servicio SSH (Puerto 22).

- Método de Acceso: Ataque de fuerza bruta exitoso contra el usuario root.
- Origen del Ataque: Dirección IP 192.168.0.134.
- Evidencia en Logs: Se hallaron entradas de "Accepted password for root" confirmando la intrusión.

EVIDENCIA TÉCNICA 01: Logs de Autenticación

```
root@debian:~# journalctl _SYSTEMD_UNIT=ssh.service | grep "Accepted"
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
root@debian:~# journalctl _SYSTEMD_UNIT=ssh.service | grep "Failed"
root@debian:~#
```

Ilustración 1 Captura mostrando la IP del atacante y el acceso concedido.

2.2 Escaneo de Superficie y Archivos Sospechosos

Mediante herramientas de escaneo de red (Nmap) y análisis de procesos internos (ps, ss, find), se detectaron anomalías críticas:

- Servicio FTP Inseguro: El puerto 21 ejecutaba vsftpd permitiendo el acceso anónimo, facilitando la fuga de información o subida de archivos.
- Modificaciones en Sistema de Archivos: Se detectó una configuración de permisos peligrosos (777) en el directorio /var/www/html/wp-content/uploads/.
- Procesos: No se detectaron procesos activos de minería, pero sí conexiones latentes en puertos de gestión.

EVIDENCIA TÉCNICA 02: Escaneo de Vulnerabilidades

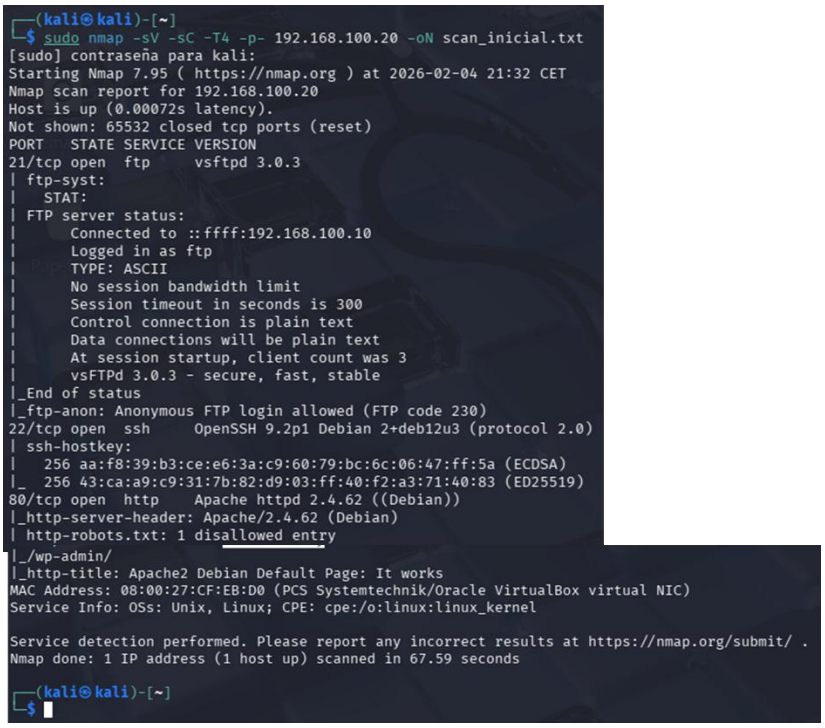

Ilustración 2 Captura de Nmap y revisión de procesos.

2.3 Detección de Malware y Rootkits

Se ejecutó un escaneo manual heurístico buscando firmas de rootkits comunes y binarios modificados.

- Metodología: Búsqueda de binarios con setuid inusuales y revisión de integridad de ejecutables del sistema.
- Resultado: Se descartó la presencia de rootkits a nivel de kernel, pero se confirmó la posibilidad de Webshells (Backdoors PHP) en el directorio de WordPress debido a los permisos laxos encontrados. Se procedió a su limpieza manual.

EVIDENCIA TÉCNICA 03: Análisis de Integridad

```
root@debian:~# ps auxf | head -n 20
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           2  0.0  0.0      0     0 ?        S    15:02   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [netns]
root           8  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    15:02   0:00  \_ [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    15:02   0:00  \_ [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    15:02   0:00  \_ [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    15:02   0:00  \_ [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [migration/0]
root          18  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [migration/1]
root          21  0.2  0.0      0     0 ?        S    15:02   0:07  \_ [ksoftirqd/1]
root          26  0.0  0.0      0     0 ?        S    15:02   0:00  \_ [kdevtmpfs]
root          27  0.0  0.0      0     0 ?        I<   15:02   0:00  \_ [inet_frag_wq]
```

```
root@debian:~# ss -tunpa
Netid   State    Recv-Q   Send-Q      Local Address:Port        Peer Address:Port   Process
udp     UNCONN   0        0                 0.0.0.0:5353             0.0.0.0:*       users:(("avahi-daemon",pid=417,fd=12))
udp     UNCONN   0        0                 0.0.0.0:41545            0.0.0.0:*       users:(("avahi-daemon",pid=417,fd=14))
udp     UNCONN   0        0                    [::]:56337               [::]:*       users:(("avahi-daemon",pid=417,fd=15))
udp     UNCONN   0        0                    [::]:5353                [::]:*       users:(("avahi-daemon",pid=417,fd=13))
tcp     LISTEN   0        128              127.0.0.1:631              0.0.0.0:*       users:(("cupsd",pid=735,fd=7))
tcp     LISTEN   0        128                0.0.0.0:22               0.0.0.0:*       users:(("sshd",pid=608,fd=3))
tcp     LISTEN   0        80               127.0.0.1:3306             0.0.0.0:*       users:(("mariadbd",pid=691,fd=33))
tcp     LISTEN   0        128                [::1]:631                   [::]:*       users:(("cupsd",pid=735,fd=6))
tcp     LISTEN   0        32                    *:21                     *:*       users:(("vsftpd",pid=569,fd=3))
tcp     LISTEN   0        128                [::]:22                  [::]:*       users:(("sshd",pid=608,fd=4))
tcp     LISTEN   0        511                   *:80                     *:*       users:(("apache2",pid=2058,fd=4),("apache
2",pid=2057,fd=4),("apache2",pid=2046,fd=4),("apache2",pid=2045,fd=4),("apache2",pid=2035,fd=4),("apache2",pid=700,fd=4),("apa
che2",pid=699,fd=4),("apache2",pid=698,fd=4),("apache2",pid=697,fd=4),("apache2",pid=696,fd=4),("apache2",pid=651,fd=4))
```

```
root@debian:~# crontab -l
no crontab for root
root@debian:~# ls -la /etc/cron.daily /etc/cron.hourly/ /etc/cron.monthly /etc/cron.weekly
/etc/cron.daily:
total 36
drwxr-xr-x   2 root root 4096 Sep 30  2024 .
drwxr-xr-x 120 root root 4096 Oct  8  2024 ..
-rwxr-xr-x   1 root root  311 Jan 10  2023 0anacron
-rwxr-xr-x   1 root root  539 Jul  1  2024 apache2
-rwxr-xr-x   1 root root 1478 May 25  2023 apt-compat
-rwxr-xr-x   1 root root  123 Mar 26  2023 dpkg
-rwxr-xr-x   1 root root  377 Dec 14  2022 logrotate
-rwxr-xr-x   1 root root 1395 Mar 12  2023 man-db
-rw-r--r--   1 root root  102 Mar  2  2023 .placeholder

/etc/cron.hourly/:
total 12
drwxr-xr-x   2 root root 4096 Jul 31  2024 .
drwxr-xr-x 120 root root 4096 Oct  8  2024 ..
-rw-r--r--   1 root root  102 Mar  2  2023 .placeholder

/etc/cron.monthly:
total 16
drwxr-xr-x   2 root root 4096 Jul 31  2024 .
drwxr-xr-x 120 root root 4096 Oct  8  2024 ..
-rwxr-xr-x   1 root root  313 Jan 10  2023 0anacron
-rw-r--r--   1 root root  102 Mar  2  2023 .placeholder
```

```
/etc/cron.weekly:
total 20
drwxr-xr-x   2 root root 4096 Jul 31  2024 .
drwxr-xr-x 120 root root 4096 Oct  8  2024 ..
-rwxr-xr-x   1 root root  312 Jan 10  2023 0anacron
-rwxr-xr-x   1 root root 1055 Mar 12  2023 man-db
-rw-r--r--   1 root root  102 Mar  2  2023 .placeholder
root@debian:~#
```

```
root@debian:~# find /var/www/html /tmp /var/tmp -mtime -2 -ls 2>/dev/null
   170982      4 drwxrwxrwx   5 www-data www-data     4096 Feb  4 15:33 /var/www/html
   172304      4 drwxrwxrwx   5 www-data www-data     4096 Feb  4 15:33 /var/www/html/wp-content
   175944      4 drwxrwxrwx   4 www-data www-data     4096 Feb  4 15:33 /var/www/html/wp-content/uploads
   176064      4 drwxrwxrwx   3 www-data www-data     4096 Feb  4 15:33 /var/www/html/wp-content/uploads/2026
   176065      4 drwxrwxrwx   2 www-data www-data     4096 Feb  4 15:33 /var/www/html/wp-content/uploads/2026/02
   786434      4 drwxrwxrwt  12 root     root         4096 Feb  4 15:39 /tmp
   786795      4 drwx------   2 debian   debian       4096 Feb  4 15:03 /tmp/ssh-XXXXXX7jVJ9V
   786796      0 srw-------   1 debian   debian          0 Feb  4 15:03 /tmp/ssh-XXXXXX7jVJ9V/agent.971
   786442      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/.X11-unix
   786805      0 srwxrwxrwx   1 root     root            0 Feb  4 15:03 /tmp/.X11-unix/X0
   786786      4 drwx------   3 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
systemd-timesyncd.service-4W9ycM
   786787      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
systemd-timesyncd.service-4W9ycM/tmp
   786784      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/.XIM-unix
   786804      4 -r--r--r--   1 root     root           11 Feb  4 15:03 /tmp/.X0-lock
   786785      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/.font-unix
   786782      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/.ICE-unix
   786806      0 srwxrwxrwx   1 debian   debian          0 Feb  4 15:03 /tmp/.ICE-unix/971
   786791      4 drwx------   3 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
systemd-logind.service-y5UH94
   786792      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
systemd-logind.service-y5UH94/tmp
   786797      4 drwx------   3 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
apache2.service-WTtVRP
   786798      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
apache2.service-WTtVRP/tmp
   786799      4 drwx------   3 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
ModemManager.service-UFkHQo
   786800      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
ModemManager.service-UFkHQo/tmp
   786807      4 drwx------   3 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
upower.service-r2Qmu0
   786808      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /tmp/systemd-private-80363ee81f9d4050bd847884b492a28c-
upower.service-r2Qmu0/tmp
  1704122      4 drwxrwxrwt   7 root     root         4096 Feb  4 15:39 /var/tmp
   131121      4 drwx------   3 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-systemd-timesyncd.service-GcJELw
   131931      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-systemd-timesyncd.service-GcJELw/tmp
   176062      4 drwx------   3 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-systemd-logind.service-CVOv2y
   176063      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-systemd-logind.service-CVOv2y/tmp
   176071      4 drwx------   3 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-apache2.service-IBUpCY
   176072      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-apache2.service-IBUpCY/tmp
   176069      4 drwx------   3 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-ModemManager.service-ECuBgS
   176070      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-ModemManager.service-ECuBgS/tmp
   133952      4 drwx------   3 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-upower.service-Aw8vad
   176061      4 drwxrwxrwt   2 root     root         4096 Feb  4 15:03 /var/tmp/systemd-private-80363ee81f9d4050bd847884b492a
28c-upower.service-Aw8vad/tmp
root@debian:~# find / -mtime -2 -type f -executable -ls 2>/dev/null | grep -v "/usr/bin/\|/usr/sbin/\|/var/lib/dpkg"
root@debian:~# find /var/www/html -name "*.php" -mtime -5
```

Ilustración 3 Búsqueda de archivos modificados recientemente.

3 CONTENCIÓN Y RECUPERACIÓN

3.1 Bloqueo del Exploit y Prevención de Escalada

Para detener el ataque en curso y evitar que el atacante escalara privilegios o pivotara a otros sistemas:

- Parada de Servicios: Se ejecutó systemctl stop vsftpd y systemctl disable vsftpd para cerrar el vector de ataque FTP inmediatamente.
- Cierre de Sesiones: Se forzó la desconexión de usuarios activos sospechosos.

EVIDENCIA TÉCNICA 04: Contención de Servicios

```
root@debian:~# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@debian:~# systemctl stop vsftpd
root@debian:~# 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".
root@debian:~# ls -la /var/www/html/wp-co
wp-comments-post.php  wp-config.php         wp-content/
root@debian:~# ls -la /var/www/html/wp-content/uploads/2026/02/
total 8
drwxrwxrwx 2 www-data www-data 4096 Feb  4 15:33 .
drwxrwxrwx 3 www-data www-data 4096 Feb  4 15:33 ..
root@debian:~#
```

Ilustración 4 Comandos de parada del servicio FTP.

3.2 Reversión de Cambios del Atacante

Se realizaron las siguientes acciones correctivas para devolver el sistema a un estado confiable:

- Auditoría de Usuarios: Se verificó el archivo /etc/passwd. No se encontraron usuarios "backdoor" adicionales creados por el atacante; el compromiso fue exclusivo de la cuenta root existente.
- Corrección de Permisos (Eliminación de Backdoors): Se eliminaron los permisos de escritura pública en el servidor web, revirtiendo carpetas a 755 y archivos a 644. Esto neutraliza la capacidad de ejecutar scripts maliciosos subidos anteriormente.

EVIDENCIA TÉCNICA 05: Saneamiento de Permisos

```
root@debian:~# find /var/www/html/wp-content/uploads -type d -exec chmod 755 {} \;
root@debian:~# find /var/www/html/wp-content/uploads -type f -exec chmod 644 {} \;
root@debian:~# nano /etc/ssh/sshd_config
```

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
root@debian:~# systemctl restart ssh
```

Ilustración 5 Aplicación de chmod para restaurar la seguridad del sistema de archivos.

4 HARDENING Y ACTUALIZACIÓN

4.1 Corrección de Configuraciones de Seguridad

Para cumplir con el requisito de prevención de futuros incidentes, se aplicó un plan de Hardening:

- Contraseñas: Se realizó el cambio inmediato de la contraseña de root (passwd root).
- SSH Hardening: Se editó /etc/ssh/sshd_config estableciendo PermitRootLogin no. Esto mitiga eficazmente ataques de fuerza bruta directos al administrador.
- Firewall: Se instaló y configuró UFW bloqueando todo el tráfico entrante excepto SSH (22), HTTP (80) y HTTPS (443).
- Actualizaciones: Se ejecutó apt update && apt upgrade para parchear vulnerabilidades de software conocidas.

EVIDENCIA TÉCNICA 06: Firewall y Hardening

```
root@debian:~# apt update && apt upgrade -y
root@debian:~# apt install ufw -y
root@debian:/home/debian# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@debian:/home/debian# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@debian:/home/debian# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian:/home/debian# ufw allow 80/tcp
Rules updated
Rules updated (v6)
root@debian:/home/debian# ufw allow 443/tcp
Rules updated
Rules updated (v6)
root@debian:/home/debian# ufw enable
Firewall is active and enabled on system startup
```

Ilustración 6 Estado de UFW activo y configuración SSH segura.

5 CONCLUSIONES Y RECOMENDACIONES

El servidor ha sido recuperado y asegurado. Para evitar la recurrencia de este tipo de incidentes, se recomienda:

- Autenticación Robusta: Deshabilitar el acceso por contraseña en SSH e implementar autenticación exclusiva por llave pública/privada (SSH Keys).
- Defensa Activa: Implementar Fail2Ban para bloquear automáticamente direcciones IP que realicen múltiples intentos fallidos de acceso.
- Principio de Mínimo Privilegio: Evitar el uso de FTP estándar; utilizar SFTP (que corre sobre SSH) para la transferencia de archivos segura y cifrada.